MODULE CODE &NAME: NEWNF401 NETWORK FUNDAMENTALS

COMPETENCE: APPLY NETWORK FUNDAMENTALS

REQF Level: 4 **Learning hours:120**

Credits: 12

Sector: ICT **Sub-sector: Networking**

Elements of competence	Performance criteria
1. Introduce Network Concepts	1.1.Proper description of Network concepts and technologies 1.2.Proper description of Network topology 1.3.Adequate study of network devices, components and their functions
2. Apply network protocols and communications	1.1.Correct description of Network Protocols 1.2.Appropriate description of Network standards 1.3.Appropriate identification and application of Network media
3. Apply IP addressing(IP v4&IPv6)	3.1.Correct description of IP addressing concepts 3.2.Convenient application of IPv4 (Internet protocol version 4) 3.3.Convenient application of IPv6 (Internet protocol version 6)

LEARNING UNIT 1=10Hours

Introduce Network Concepts

Learning Outcomes:

1. Describe Network concepts and technologies

2. Describe Network topology

3. Study network devices, components and their functions

Learning Outcome1.1: Describe Network concepts and technologies

Definition of computer network

1.Computer Network Definition

A **computer network** is a system of interconnected computers for the purpose of sharing data and resources

Computers on a network are called nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two devices are networked together when one device is able to exchange information with the other device. The computer can be connected to another in the two ways.

Wired network: Computers are connected using cable media. Most commonly Ethernet Cable, coaxial cable and optic fiber.

Wireless network: Computers are connected using wireless media. Radio waves are used in wireless mode.

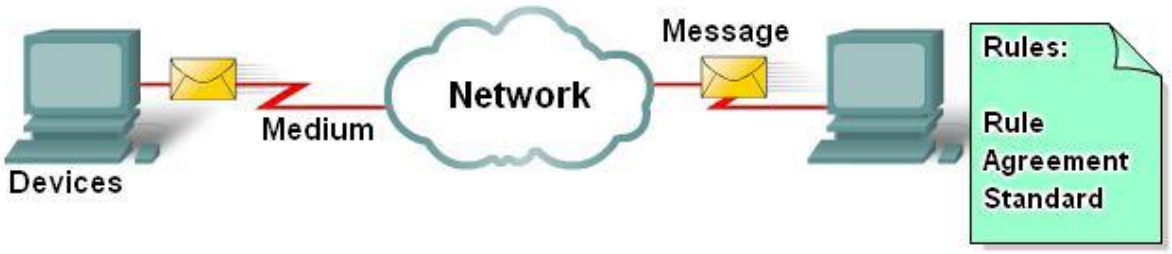
Networking is the practice of linking two or more computing devices together for the purpose of sharing data. Networks are built with a mix of computer hardware and computer software.

2 Properties of Computer Network

- **Easy Sharing of Resources:** Computers are able to share various resources easily over a network. Shared resources can be Internet, files, printer, storage and others.
- **Performance:** It is achieved by measuring the speed of data transmission with number of network users, connectivity used and the software used. The commonly measured qualities in the network performance are **Bandwidth** and **Latency**.
- **Reliability:** It means that computer network provides assurance of the delivery of data to the intended recipient.
- **Scalability:** The possibility of adding new computer without affecting the network performance.
- **Security:** computer network must be secured for the benefit of the user and data protection. The security is achieved by protecting data from unauthorized access.
- **Quality of Service (QoS):** Quality of Service refers to the mechanism that manage congested network traffic.
- **Fault tolerant**: A fault tolerant network limits the impact of hardware or software failure and recovers quickly when a failure occurs

2. Elements of network

The Elements of network



Four elements of a network:

- Rules
- Medium
- Messages
- Devices

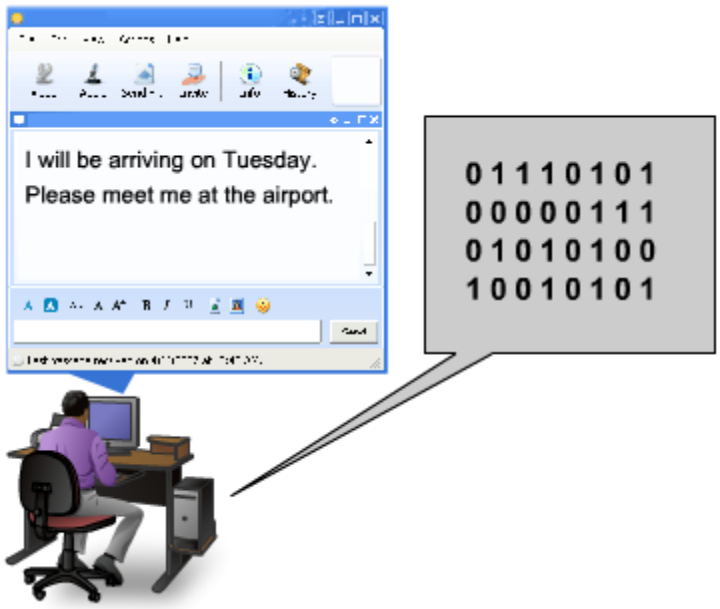
There Four Elements of a Network

1.Rules or agreements to govern the messages are sent, directed, received and interpreted

i.e A set of rules governing how to communicate (protocols).

2.The *messages* or units of information that travel from one device to another i.e A resource to share. Messages

- Message is a generic term that encompasses text, voice or video information
- The message must be converted to *bits*, binary coded digital signals, before they are transmitted on the medium



3. Medium

- Physically carries the message
- Connects the devices
- Can be wired or wireless

A means of interconnecting these devices – a *medium* that can transport the messages from one device to another i.e A pathway to transfer data (transmission medium)

4.Devices on the network that exchange messages with each other

Network devices classification

Interconnection devices

Access devices

End devices

End Devices

The network devices that people are most familiar with are called end devices.
Some examples of end devices are:
Computers (work stations, laptops, file servers, web servers)
Network printers
VoIP phones
Security cameras
Mobile handheld devices (such as wireless barcode scanners, PDAs)

In the context of a network, end devices are referred to as hosts. A host device is either the
source or destination of a message transmitted over the network.

Intermediate devices

In addition to the end devices that people are familiar with, networks rely on intermediary devices to provide connectivity
devices connect the individual hosts to the network and can connect multiple individual networks
to form an internetwork.
Examples of intermediary network devices are:
Network Access Devices (Hubs, switches, and wireless access points)
Internetworking Devices (routers)
Communication Servers and Modems
Security Devices (firewalls

3. Network benefits

BENEFITS OF COMPUTER NETWORK

(1) Computers which are connected through a network can share resources as hard drives, printers, scanners etc with each other.
(2) They can send file from one computer to another quite easily.
(3) You can connect all the computers which are connected through a network to the internet by using a single line. So it means that you can save the connection cost for each computer but you internet connection must be fast.
(4) IF you want to access data from the other computer which is the part of network then you can access data from that computer.
(5) Users can run those programs which are not installed on their computers but are installed on any other user's computer

1. **Enhanced communication and availability of information:** It allows access to a vast amount of useful information.
   - **Example**: Population data, newsletters, online businesses, contents, Applications.
2. **Allow resource sharing:** Fewer resources are needed when an organization uses a computer network.
   - **Example:** only one printer is needed instead of buying a printer for each office.
3. **File sharing made easy:** computer network allows people to share files, which helps to save more time and effort.
   - **Example:** A teacher can share homework to all students through school network

4. **Improve storage capacity:** since you are going to share information, files and resources to other people, you have to ensure that all data and content are properly stored in the system.
5. **Cost efficiency:** on computer network, you can share software license installed on the server and can then be used by various workstations.
6. **Security of information and resources:** users cannot see other users' files unlike on stand-alone machines.
7. ***Backup of data* is easy** as all the data is stored on the file server.

Disadvantages of Computer Networks

- **Security Issues**: One of the major drawbacks of computer networks is the security issues involved. If a computer is a standalone, physical access becomes necessary for any kind of data theft. However, if a computer is on a network, a computer hacker can get unauthorized access by using different tools. In case of big organizations, various network security softwares are used to prevent the theft of any confidential and classified data.
- **Rapid Spread of Computer Viruses**: If any computer system in a network gets affected by computer virus, there is a possible threat of other systems getting affected too. Viruses get spread on a network easily because of the interconnectivity of workstations. Such spread can be dangerous if the computers have important database which can get corrupted by the virus.
- **Expensive Set Up**: The initial set up cost of a computer network can be high depending on the number of computers to be connected. Costly devices like routers, switches, hubs, etc., can add up to the bills of a person trying to install a computer network. He will also have to buy NICs (Network Interface Cards) for each of the workstations, in case they are not inbuilt.
- **Dependency on the Main File Server**: In case the main File Server of a computer network breaks down, the system becomes useless. In case of big networks, the File Server should be a powerful computer, which often makes it expensive.
- **Lack of independence**: people rely on computer network and when the system is down, people get stack. Most of organizations depend on the computer networks.
- **Security issues:** huge number of people use a computer network to get and share their files and resources, a certain user's security would be always at risk. Viruses can spread to other computers throughout a computer network. There is a danger of

hacking, particularly with wide area networks. Security procedures are needed to prevent such abuse, Examples: The use of Antivirus and firewall.

- **Lack of robustness:** computer network's main server breaks down, the entire system would become useless

Network Criteria

- Performance
- It can be measured in many ways, including transmit time and response time. Transmit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
- Performance of a network depends upon the factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

✓ Performance is often evaluated by two networking metrics: Throughput and delay.

- Reliability

✓ Network reliability is measured by the frequency of failure, the time it takes to recover from a failure, and the network's robustness in a catastrophe.

- Security

✓ It includes protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedure for recovery from breaches and data loses.

3.1.1 Network metrics

Network metrics are defined as standards of measurement by which efficiency, performance, progress, or quality of a plan, process can be assessed. Network metric are used by a router to make routing decisions.

When data is sent over a computer network, it is broken up into small chunks called **packets.** Each packet contains source and destination address information. Packets are sent across a network one bit at a time.

a. ***Bandwidth***

Bandwidth is the amount of data that can be transmitted in a fixed amount of time. Bandwidth is measured in the number of bits that can be sent every second.

The following are examples of bandwidth measurements:

- b/s - bits per second
- kb/s - kilobits per second
- Mb/s - megabits per second
- Gb/s - gigabits per second

b. Latency

Latency is the time between requesting data and receiving data. More simply put, the time it takes to establish a connection between your computer and the server hosting the website you requested. The important thing to take away here is that latency is not speed. Data is delayed by network devices and cable length. Network devices add latency when processing and forwarding data.

c. Throughput:

Throughput is the actual rate at which information is transferred. It measures the amount of completed work against time consumed and may be used to measure the performance of a processor, memory and/or network communications.

d. Error rate:

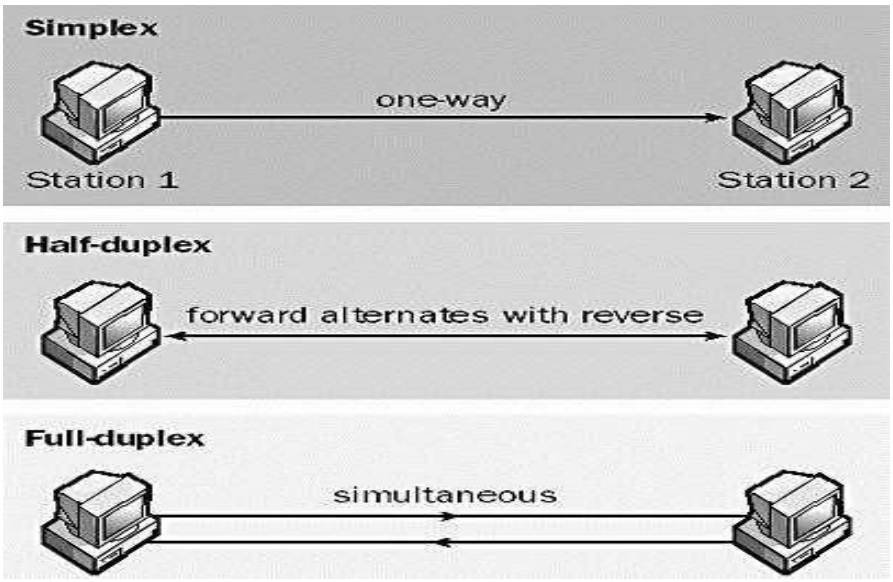
Error rate is the number of corrupted bits expressed as percentage or fraction of the total sent.

e. Jitter:

Jitter is variation in packet delay at the receiver of information. For measuring the capacity of all of these metrics above, we focus on capacity of message and this one change into different form depending on the network devices where this message is located.

Data Transmission model

The term transmission mode is used to define the direction of signal flow between two linked devices. The data that is transmitted over the network can flow using one of three modes: simplex, half-duplex and full-duplex.



Picture 3. 6: Transmission modes: simplex, half-duplex and full-duplex

1. **Simplex:** it is a single one-way transmission. In a **simplex transmission mode**, the communication between sender and receiver occurs only in one direction. That means only the sender can transmit data, and receiver can receive that data. The receiver cannot transmit any information back to the sender.

Picture 3. 7: Keyboard to monitor is an example of simplex transmission mode.

Example of simplex transmission:

- Communication between a computer and a printer
- Listening to the radio
- The signal that is sent from a TV station to your home TV.

2. Half-Duplex: data flows in one direction at a time. In half-duplex, the channel of communications allows alternating transmission in two directions, but not in both directions simultaneously.

Picture 3. 8: Example of Half-duplex is the Talkie- Walkie used by the police.

4. **Full-Duplex:** data flows in both directions at the same time. In a **full duplex transmission mode**, the communication between sender and receiver can occur simultaneously. Sender and receiver both can transmit and receive simultaneously at the same time.

Basis for Comparison	**Simplex**	**Half Duplex**	**Full Duplex**
Direction of Communication	Communication is unidirectional.	Communication is twodirectional but, one at a time.	Communication is two directional and done simultaneously.
Send/Receive	A sender can send data but, cannot receive.	A sender can send as well as receive the data but one at a time.	A sender can send as well as receive the data simultaneously.
Performance	The half-duplex and full duplex produces better performance than the Simplex.	The full duplex mode produces higher performance than half duplex.	Full duplex has better performance as it doubles the utilization of bandwidth.
Example	Keyboard and monitor.	Walkie-Talkies, internet chart	Telephone.

Table 3.1: *comparison of network transmission modes*

A telephone conversation is an example of full-duplex communication. Both people can talk and be heard at the same time.

Distinguishing between network classification

Classifying network by components roles

Peer to peer network

Client/server network

Local Area Networks (LANs)

Definition

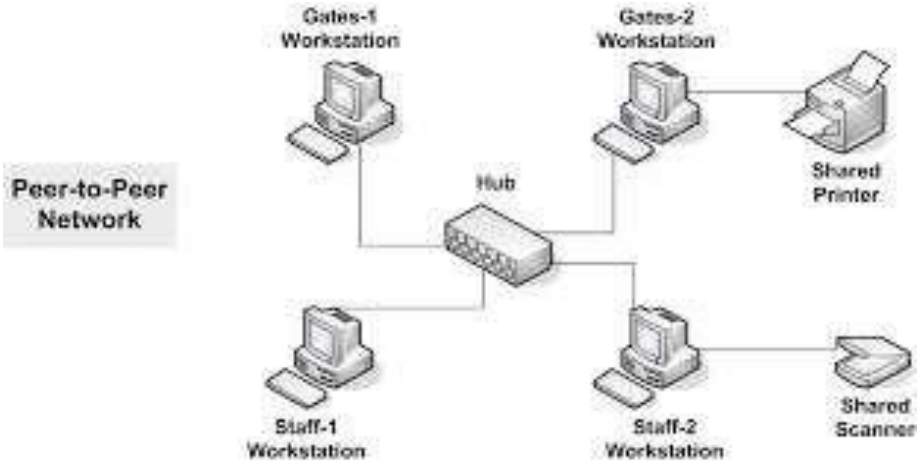
Local Area Networks (LANs) are networks usually confined to a geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people.

LAN Categories

1. Peer-to-Peer Network

A peer-to-peer (P2P) network is created when two or more computers are connected and share resources without going through a separate server computer. In a peer-to-peer network, there is no hierarchy among the computers, nor are there any dedicated servers.

Each device on the network, also called a client, has equivalent capabilities and responsibilities. A user is responsible for its own resources and can decide which data and devices to be shared with other computers. Because individual users are responsible for the resources on their own computers, the network has no central point of control and no central administration. Peer-to-peer networks work best in environments with ten or fewer computers.



: Peer-to-Peer network

Advantages of peer to peer network are as follows:

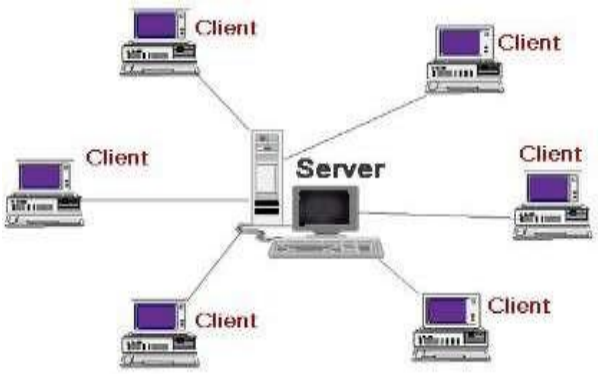
- The main advantage of peer to peer network is that it is easier to set up
- In peer-to-peer networks all nodes are act as server as well as client therefore no need of dedicated server
- The peer to peer network is less expensive
- Peer to peer network is easier to set up and use this means that you can spend less time in the configuration and implementation of peer to peer network.

Disadvantages of peer to peer network

- A computer can be accessed anytime
- Network security has to be applied to each computer separately
- Backup has to be performed on each computer separately
- No centralized server is available to manage and control the access of data.

2. **Client-Server Network**

In a client-server network, the client requests information or services from the server and the server provides the requested information or service to the client. Servers on a client-server network commonly perform some of the processing work for client machines.



Client-Server Network

In a client-server network, resources are controlled by a centralized network administration. The network administrator implements data backups and security measures. The network administrator also controls user access to the server resources.

Note: In a home or small business, a single server can run multiple types of server software, it may be necessary for one computer to act as a file server, a web server, and an email server. A client computer can also run multiple types of client software. There must

be client software for every service required. With multiple client software installed, a client can connect to multiple servers at the same time.

Advantages of Client-Server Network

- **Centralization of control:** access, resources and integrity of the data are controlled by the dedicated server so that a program or unauthorized client cannot damage the system.
- **Scalability:** You can increase the capacity of clients and servers separately. Any element can be increased (or enhanced) at any time, you can add new nodes to the network (clients or servers).
- **Easy maintenance**: distribute the roles and responsibilities to several standalone computers, you can replace, repair, upgrade, or even move a server, while customers will not be affected by that change (or minimally affect).

- The followings are main five advantages of using client/server network
- a. **centralized** means Resources and data are controlled through the server
- b. **Scalability** means that any or all elements can be replaced individually as needs increase.
- c. **Flexibility** means new technology can be easily integrated into a system.
- d. **Inter-Operability** means all components (client/network/server)work together
- e**. Accessibility** means server can be accessed remotely and across multiple platforms

Characteristics of a client over a network:

- It is the first active (or master);
- Sends requests to the server;

It expects and receives responses from the server

Characteristics of a server over a network:

- It is initially passive (or slave, waiting for a query);
- It is listening, ready to respond to requests sent by clients;
- When a request comes, he treats it and sends a response.

Disadvantage of Client Server Networks

⇒ There is a reliance on the central server, if it fails, no work can be done
⇒ A network manager is required and this costs money
⇒ The server costs money, as does the network operating system

⇒ Servers are powerful, thus expensive

⇒ Lots of network traffic.

⇒ If too many clients to communicate with the server at the same time, it may not carry the load (while peer to peer networks work better by adding new members).

⇒ If the server is no longer available, most customers do not walk (the peer network continues to function even if many participants leave the network).

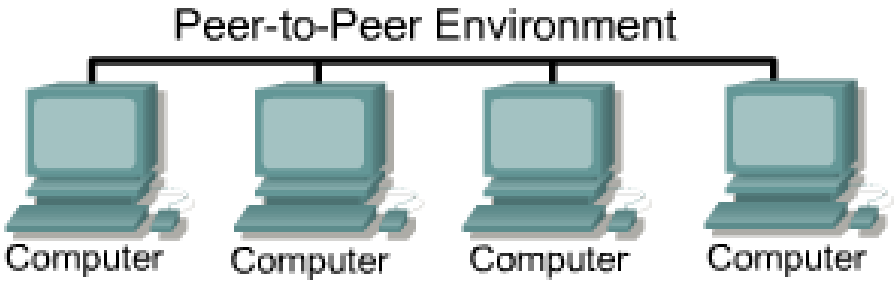
⇒ The costs of setting up and maintenance are high

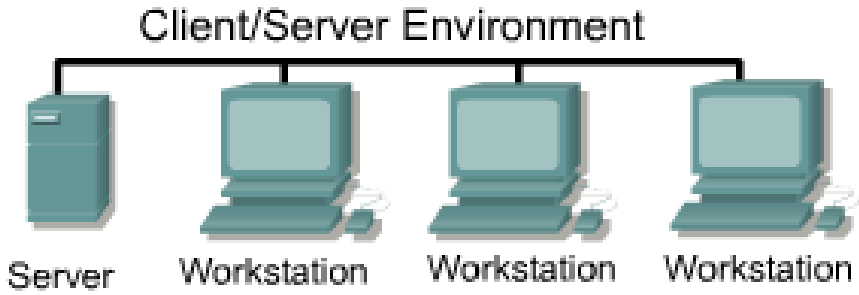
Advantages of Client Server Networks over Peer to Peer Networks

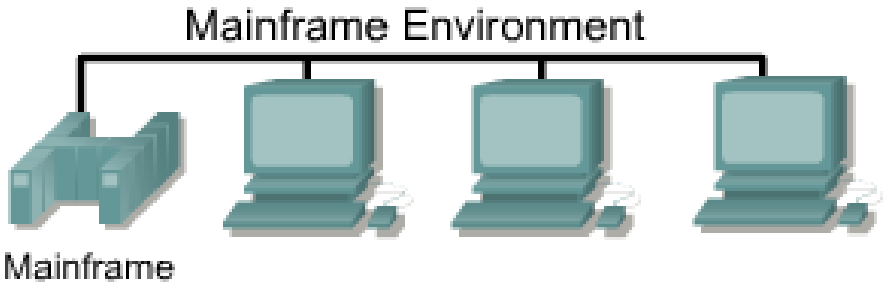
- **Centralization:** Unlike Peer to Peer, where there is no central administration, Client Server Networks have a centralized control.
- **Proper Management :** All the files are stored at the same place. Therefore, management of files becomes easy and it is easier to find files.
- **Back-up and Recovery possible:** As all the data is stored on server it is easy to make a back-up of it. Also, in case of some break-down if data is lost, it can be recovered easily and efficiently. While in peer to peer network, we have to take back-up at every workstation.
- **Upgrade and Scalability in Client-server set-up**: Changes can be made easily by just upgrading the server. Also new resources and systems can be added by making necessary changes in server.
- **Accessibility:** From various platforms in the network, server can be accessed remotely.
- **Security:** Rules defining security and access rights can be defined at the time of set-up of server.

Disadvantages of client server network over the Peer to peer network

- **Congestion in Network:** Too many requests from the clients may lead to congestion, which rarely takes place in Peer to Peer network. Overload can lead to breaking-down of servers. In peer-to-peer, the total bandwidth of the network increases as the number of peers increase.
- Client-Server network is **not as robust** as a Peer to Peer network and if the server fails, the whole network goes down.
- **Cost:** It is very expensive to install and manage **client server network.**







3. **Centralized** - This is also a client/server based model that is most often seen in UNIX environments, but the clients are "dumb terminals". This means that the client may not have a floppy drive, hard disk or CDROM and all applications and processing occur on the server/s. As you can imagine, this requires fast and expensive server/s. Security is very high on this type of network.

Classifying network by geographical area

A computer network is classified by the following specific characteristics:

1. Size of the area covered
2. Number of users connected
3. Number and types of services available
4. Area of responsibility

Types of networks

There are about eight types of network which are used world wide these days, both in houses and commercially. These networks are used on the bases of their scale and scope, historical reasons, preferences for networking industries, and their design and implementation issues. LAN and WAN are mostly known and used widely. LAN, local area network was first invented for communication between two computers

LAN operates through cables and network cards. Later WLAN, Wireless local area network was formed through LAN concept, there are no wires involved in communication between computers, and Wireless LAN cards are required to connect to wireless network. LAN is the original network out of which other networks are formed according to requirements. They are as follow.

-LAN - Local Area Network

- WLAN - Wireless Local Area Network

- WAN - Wide Area Network

- MAN - Metropolitan Area Network

- SAN - Storage Area Network, It can also refer with names like System Area Network, Server Area Network, or sometimes Small Area Network

- CAN - Campus Area Network, Controller Area Network, and often Cluster Area Network

- PAN - Personal Area Network

- DAN - Desk Area Network

LAN - Local Area Network

LAN connects networking devices with in short spam of area, i.e. small offices, home, internet cafes etc. LAN uses TCP/IP network protocol for communication between computers. It is often but not always implemented as a single IP subnet. Since LAN is operated in short area so It can be control and administrate by single person or organization.

. Local Area Network (LAN)

Traditionally, a LAN is defined as a network that covers a small geographical area.

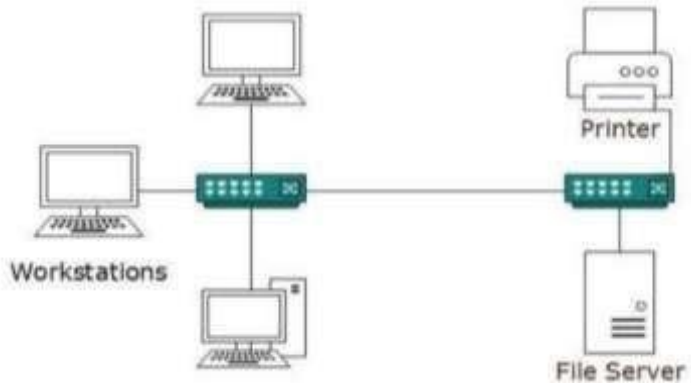
However, the distinguishing characteristic for LANs today is that they are typically owned

by an individual, such as in a home or small business, or wholly managed by an IT

department, such as in a school or corporation. This individual or group enforces the

security and access control policies of the network.

Note: *LAN uses Ethernet IEEE 802.3 as its standard.*



Graphical representation of Local Area Network

The followings are five characteristics of LAN

a. A LAN exists within a small geographical area
b. LAN cabling from end to end should not exceed 2-3 kilometers
c. LANs normally have fewer nodes about 500
d. The communication over LAN is digital because it connects computers together.
e. LAN nodes communicate at a higher speed between 4-100 Mbps

Major Components of LANs

A LAN is made of the following main components:

- Hardware:
  - ✓ Computers
  - ✓ Network interface card (NIC) linked to physical address
  - ✓ Media or Cables (Unshielded twisted pair, Coaxial cable, Optical fiber, Air for wireless)
  - ✓ Hub, Switches, repeaters
- Access Methods: Rules that define how a computer puts data on and takes it from the network cable.
- Software: Programs to access and / or to manage the network.

WAN - Wide Area Network

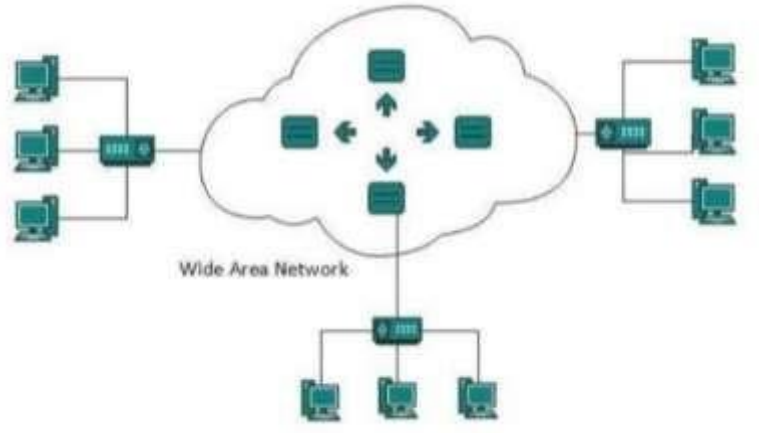
As “word” Wide implies, WAN, wide area network cover large distance for communication between computers. The Internet it self is the biggest example of Wide area network, WAN, which is covering the entire earth. WAN is distributed collection of geographically LANs. A network connecting device router

connects LANs to WANs. WAN used network protocols like ATM, X.25, and Frame Relay for long distance connectivity.

A WAN connects multiple networks that are in geographically separated locations. The distinguishing characteristic of a WAN is that it is owned by a service provider. Individuals and organizations contract for WAN services. WAN network provides connectivity to MANs and LANs. The most common example of a WAN is the Internetwork or **Internet** in short.

The **Internet** is a large WAN that is composed of millions of interconnected networks.

Example: Kigali and Nairobi networks are connected through the Internet



Graphical Representation of Wide Area Network

The followings are five characteristics of WAN

a. A WAN can be world wide

b. Government own a WAN

C. Many nodes are connected to a WAN

d. Topology used is mesh ,hierarchic or star

e. WAN transmission is digital as well as analogue

Wireless - Local Area Network

A LAN, local area network based on wireless network technology mostly referred as Wi-Fi. Unlike LAN, in WLAN no wires are used, but radio signals are the medium for communication. Wireless network cards are required to be installed in the systems for accessing any wireless network around. Mostly wireless cards connect to wireless routers for communication among computers or accessing WAN, internet.

A Wireless LAN (WLAN) is a LAN that uses radio waves to transmit data between wireless devices. In a traditional LAN, devices are connected together using copper cabling. In some environments, installing copper cabling might not be practical, desirable, or even possible. In these situations, wireless devices are used to transmit and receive data using radio waves. As with LANs, on a WLAN, you can share resources, such as files, printers, and Internet access.

Note: W*LAN uses Ethernet IEEE 802.11 as its standard.*

Advantages of wireless networks:

- Mobility - With a laptop computer or mobile device, access can be available throughout a school, at the mall, on an airplane, etc. More and more businesses are also offering free Wi-Fi access.
- Fast setup - If your computer has a wireless adapter, locating a wireless network can be as simple as clicking "Connect to a Network" -- in some cases, you will connect automatically to networks within range.
- Cost - Setting up a wireless network can be much more cost effective than buying and installing cables.
- Expandability - Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).
- Security - Wireless networks are much more susceptible to unauthorized use. If you set up a wireless network, be sure to include maximum security

Disadvantages of wireless networks

- Interference - Because wireless networks use radio signals and similar techniques for transmission, they are susceptible to interference from lights and electronic devices.
- Inconsistent connections Because of the interference caused by electrical devices and/or items blocking the path of transmission, wireless connections are not nearly as stable as those through a dedicated cable.
- Power consumption - The wireless transmitter in a laptop requires a significant amount of power; therefore, the battery life of laptops can be adversely impacted.
- Speed - The transmission speed of wireless networks is improving; however, faster options (such as gigabit Ethernet) are available via cables

MAN - Metropolitan Area Network

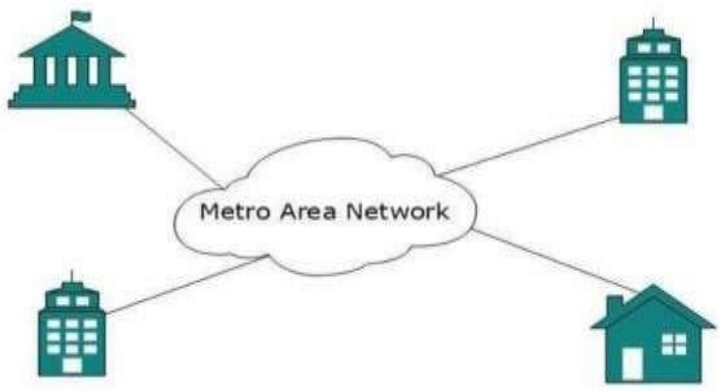
This kind of network is not mostly used but it has its own importance for some government bodies and organizations on larger scale. MAN, metropolitan area network falls in middle of LAN and WAN, It covers large span of physical area than LAN but smaller than WAN, such as a city.

A metropolitan area network (MAN) is a network that spans across a large organization like campus or a city. The network consists of various buildings interconnected through wireless or fiber optic backbones.

A ***backbone*** is the part of the computer *network* infrastructure that interconnects different LAN *networks* and provides a path for exchange of data between these different *networks*

Backbone network: A BBN is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or sub networks.

The communication links and equipment are typically owned by a network service provider who sells the service to the users. A MAN can acts as a high-speed network to enable sharing of regional resources



Graphical representation of Metropolitan Area Network

CAN - Campus Area Network

Networking spanning with multiple LANs but smaller than a Metropolitan area network, MAN. This kind of network mostly used in relatively large universities or local business offices and buildings.

SAN - Storage Area Network

SAN technology is used for data storage and it has no use for most of the organization but data oriented organizations. Storage area network connects servers to data storage devices by using Fiber channel technology

SAN - System Area Network

SAN, system area networks are also known as cluster area network and it connects high performance computers with high speed connections in cluster configuration.

Personal Area Network (PAN)

A personal area network (PAN) is a network that connects devices, such as mice, keyboards, printers, Smartphone, and tablets within the range of an individual person. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes. All of these devices are dedicated to a single host and are most often connected with Bluetooth technology.

Bluetooth is a wireless technology that enables devices to communicate over short distances. A Bluetooth device can connect up to seven other Bluetooth devices.

Representation of two devices connected by Bluetooth

INTRODUCTION TO NETWORK TECHNOLOGIES

1. IEEE802.3 Ethernet

Ethernet

Ethernet is a family of computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks. Ethernet cable is one of the most popular forms of network cable used in wired networks. They connect devices together within a local area network like PCs, routers and switches. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Ethernet uses CSMA/CD (Carrier Sense multiple Access with Collision Detection)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

In a LAN, computers transmit data to each other. Normally, there is order to follow so that two computers can not send data at the same time while they are using the same route. When it happens that two computers send messages at the same time, there is what we call data collision. Therefore, a data collision occurs when two or more computers send data at the same time. When this happens, each computer stops data transmission and waits to resend it when the cable is free. Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a set of rules determining how network devices respond to a collision.

How does the CSMA/CD work?

Let us start by taking a look at Figure 2.3

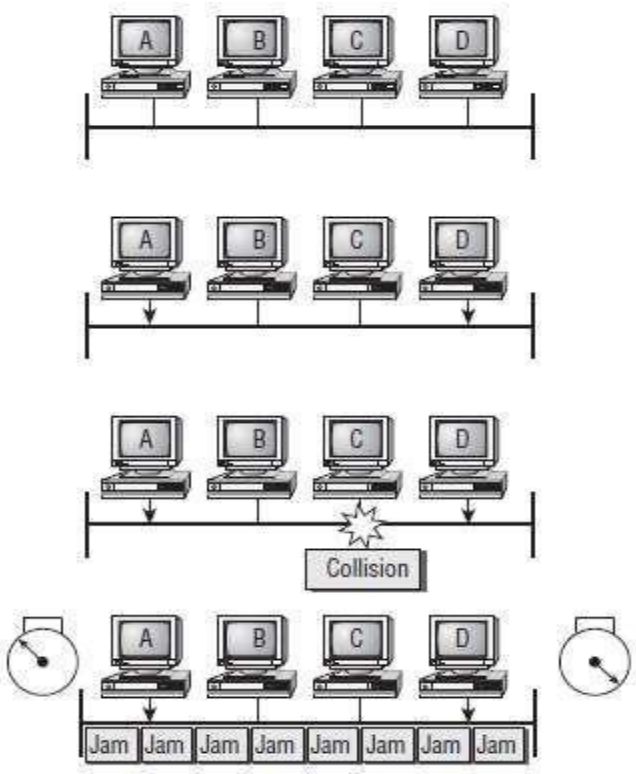


Figure 2. 2: CSMA/CD

On the figure above, host A is trying to communicate with host B. Host A "senses" the wire and decides to send data. But, in the same time, host D sends its data to host C and the collision occurs. The sending devices (host A and host D) detect the collision and resend the data after a random period of time.

When a collision occurs on an Ethernet LAN, the following happens:

 A jam signal informs all devices that a collision occurred.

A signal sent by a device on an Ethernet network to indicate that a collision has occurred on the network is called a **jam signal**.

- The collision invokes a random **backoff algorithm** (a set of rules which controls when each computer resends the data in order to assure that no more collision will happen again).
- Each device on the Ethernet segment stops transmitting for a short time until the timers expire.
- All hosts have equal priority to transmit after the timers have expired.

802.3 is a standard specification for Ethernet, a method of packet-based physical communication in a local area network (LAN), which is maintained by the Institute of Electrical and Electronics Engineers (IEEE). In general, 802.3 specifies the physical media and the working characteristics of Ethernet. The first Ethernet standards to be defined support a data rate of 10 megabits per second (Mbps) and specify these possible physical media:

10BASE5 (Thickwire coaxial cable with a maximum segment length of 500 meters)

10BASE2 (Thinwire coaxial cable with a maximum segment length of 185 meters)

10BASE-F (optical fiber cable)

10BASE-T (ordinary telephone twisted pair wire)

10BROAD36 (broadband multi-channel coaxial cable with a maximum segment length of 3,600 meters)

There are four data rates that are supported currently :-

• 10 Mbps - 10Base-T Ethernet (IEEE 802.3)

• 100 Mbps - Fast Ethernet (IEEE 802.3u)

• 1000 Mbps - Gigabit Ethernet (IEEE 802.3z)

• 10-Gigabit - 10 Gbps Ethernet (IEEE 802.3ae).

This designation is an IEEE shorthand identifier. The "10" in the media type designation refers to the transmission speed of 10 Mbps. The "BASE" refers to baseband signalling, which means that only Ethernet signals are carried on the medium (or, with 10BROAD36, on a single channel in a shared cable). The "T" represents twisted-pair; the "F" represents fiber optic cable; and the "2", "5", and "36" refer to the coaxial cable segment length in 100 meter sections (the 185 meter length has been rounded up to "2" for 200).Also see 100BASE-T and Gigabit Ethernet.

Cable Ethernet Standards

2.2.1 Definition of standard

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers in guaranteeing national and international interoperability of data and telecommunications technology and processes. With Ethernet technologies, different types of standards have been so far used in networks.

The different Ethernet technologies used in wired networks to connect computers are given in the following table. The choice of one or another type depends on the size of networks and the quantity of data to exchange.

Name	**IEEE Standard**	**Data Rate**	**Media Type**	**Maximum Distance**	**Advantages**
Ethernet	802.3	10 Mbps	10Base-T	100 meters	Low cost components
					Easy to install Easy to troubleshoot
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters	It is the most popular and cheapest Ethernet
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters	Gigabit Ethernet is ten times faster than Fast Ethernet

10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBaseSW/LW/EW	300 meters 300m Multimode Fiber (MMF) / 10km Singlemode Fiber (SMF) 10km/40km 300m/10km/40km	☐ It is the fastest one ☐ It is too expensive

10BASE-F

10BASE-F is a generic term for the family of 10 Mbit/s Ethernet standards using fiber optic cable. In 10BASE-F, the 10 represents its maximum throughput of 10 Mbit/s, BASE indicates its use of baseband transmission, and F indicates that it relies on medium of fiber-optic cable. In fact, there are at least three different kinds of 10BASE-F. All require two strands of 62.5/125 µm multimode fiber. One strand is used for data transmission and one strand is used for reception, making 10BASE-F a full-duplex technology.

The 10BASE-F variants include **10BASE-FL**, **10BASE-FB** and **10BASE-FP**. Of these only 10BASE-FL experienced widespread use. All 10BASE-F variants deliver 10 Mbit/s over a fiber pair. These 10 Mbit/s standards have been largely replaced by faster Fast Ethernet, Gigabit Ethernet and 100 Gigabit Ethernet standards.

10BASE-FL

10BASE-FL is the most commonly used 10BASE-F specification of Ethernet over optical fiber. In 10BASE-FL, FL stands for fiber optic link. It replaces the original fiber-optic inter-repeater link (FOIRL) specification, but retains compatibility with FOIRL-based equipment. The maximum segment length supported is 2000 meters. When mixed with FOIRL equipment, maximum segment length is limited to FOIRL's 1000 meters.

Today, 10BASE-FL is rarely used in networking and has been replaced by the family of Fast Ethernet, Gigabit Ethernet and 100 Gigabit Ethernet standards.

10BASE-FB

The 10BASE-FB (10BASE-FiberBackbone) is a network segment used to bridge Ethernet hubs. Due to the synchronous operation of 10BASE-FB, delays normally associated with Ethernet repeaters are reduced, thus allowing segment distances to be extended without compromising the collision detection mechanism. The maximum allowable segment length for 10BASE-FB is 2000 meters.

10BASE-FP

10BASE-FP calls for a non-powered signal coupler capable of linking up to 33 devices, with each segment being up to 500m in length. This formed a star-type network centered on the signal coupler. There are no devices known to have implemented this standard.

IEEE802.5 Token ring

The IEEE defines in the 802.5 standard , what we call the Token Ring network. As it is seen there are two words in the name of the protocol. Token and Ring. Ring is there because the computers or networking devices are connected in the form of a ring . It means that all the computers are connected to exactly two other computers on the network. Any computer is connected to the computer on its left and its right on the network . There are no other direct connections. The word Token means that the computers use the Token system for transmission. That is any computer can transmit when it is in possession of a token, which is a permission to transmit. Otherwise the computers cannot transmit. One of the disadvantages is that all the messages have to pass through all the computers falling in the path. It drastically decreases the speed of communication . Suppose for example there is a Token Ring Network of 20 computers. Now computer no 2 has to transmit to computer no 12 . All the data intended for computer no 12 has to go through all the 10 computers in between. This brings down the transmission speed and eats up valuable bandwidth.

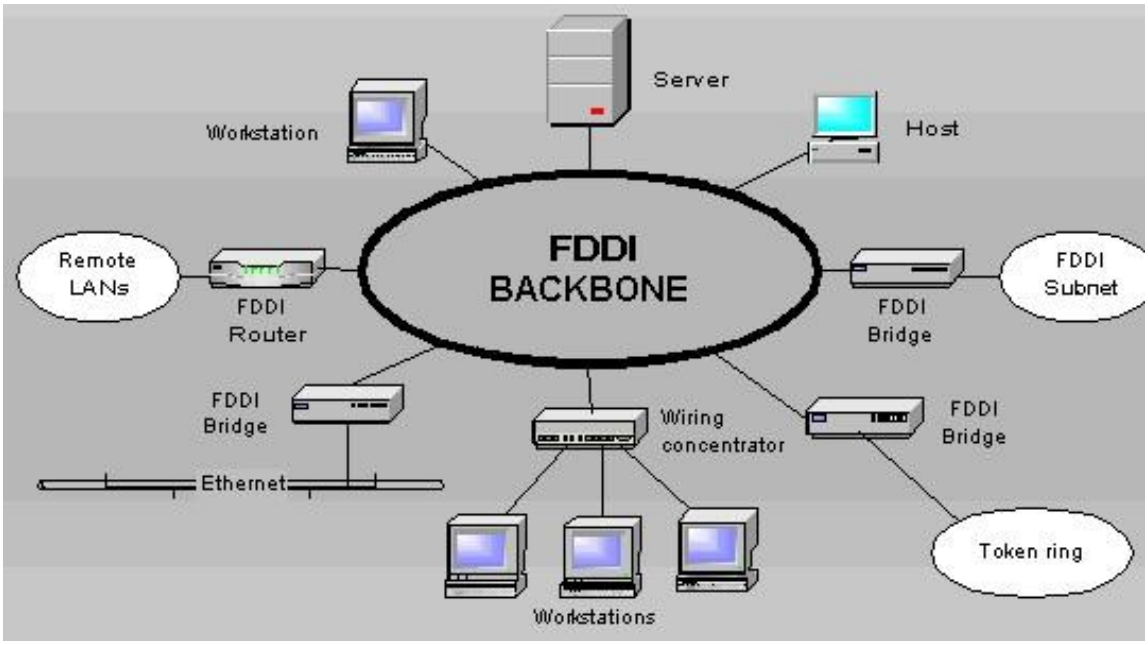
IEEE802.8 Fiber optic

Fiber Distributed Data Interface (FDDI)

Definition

The Fiber Distributed Data Interface (FDDI) is a standard developed by the American National Standards Institute (ANSI) for transmitting data on optical fiber cables. FDDI supports transmission rates of 100 megabits per second on token-passing networks.

FDDI provides high-speed network backbones that can be used to connect and extend LANs.



Fiber Distributed Data Interface LAN configuration

Advantages of FDDI

The Fiber Distributed Data Interface allows the transmission of very large volumes of data over large distances. It provides high bandwidth.

2.3.3 Disadvantages

The Fiber Distributed Data Interface (FDDI) is an expensive technology to set up because the network devices require a special network card and also the required fiber-optic cabling is expensive than twisted-pair cable. Because most Fiber Distributed Data Interface (FDDI) installations use a redundant second ring, more cabling is required.

2.3.4 Fiber Optic cables

A fiber optic cable is a glass or plastic strand that transmits information using light and is made up of one or more optical fibers enclosed together in a sheath or jacket. It has the following properties:

 Not affected by electromagnetic or radio frequency interference.

- All signals are converted to light pulses to enter the cable, and converted back into electrical signals when they leave it.
- Signals are clearer, can go farther, and have greater bandwidth than with copper cable. Signal can travel several miles or kilometers before the signal needs to be regenerated.

Usually more expensive to use than copper cabling and the connectors are more costly and harder to assemble.

- Common connectors for fiber-optic networks are SC, ST, and LC. These three types of fiber optic connectors are half-duplex, which allows data to flow in only one direction. Therefore, two cables are needed.

a) Types of fiber optic

There are three types of fiber optic cable commonly used: **single mode, multimode and plastic optical fiber (POF)**.

1. **Single-mode**: Cable that has a very thin core. It is harder to make, uses lasers as a light source, and can transmit signals dozens of kilometers with ease.

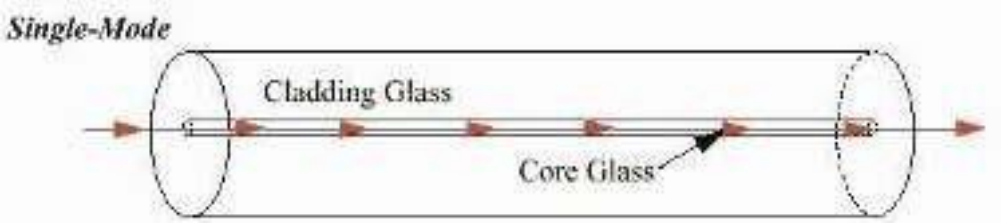


Figure 2. 6: Single mode Optical Fiber

1. **Multimode**: Cable that has a thicker core than single-mode cable. It is easier to make, can use simpler light sources (LEDs), and works well over distances of a few kilometers or less.

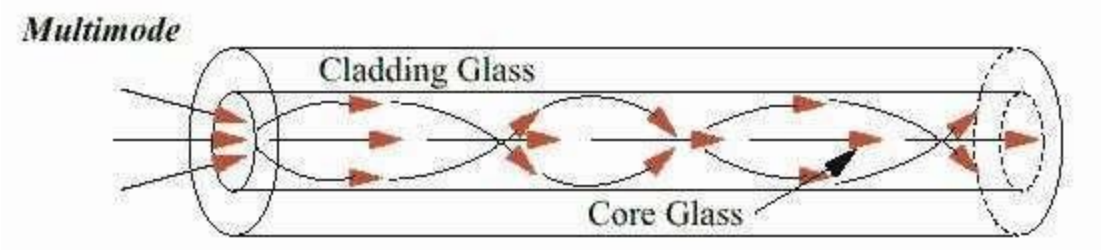


Figure 2. 7: Multimode Optical Fiber

1. Plastic optical fiber (POF): Transparent glass or plastic fibers which allow light to be guided from one end to the other with minimal loss.

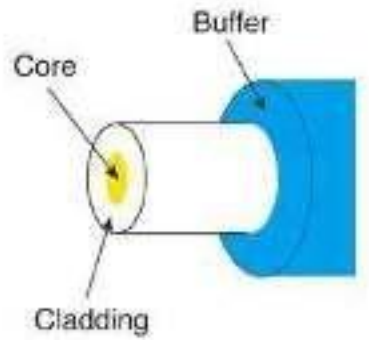


Figure 2. 8: Plastic Optical Fiber

The Fiber optic technologies are summarized in the following table.

Designation	**Supported Media**	**Maximum Segment Length**	**Transfer Speed**	**Topology**
100Base-FX	Fiber-optic- two strands of multimode 62.5/125 fiber	412 meters (Half-Duplex), 2000 m (full-duplex)	100 Mbps, (200 Mb/s full-duplex mode)	Star(often only point-to-point)
1000Base-SX	Fiber-optic- two strands of multimode 62.5/125 fiber	260m	1Gbps	Star, using buffered distributor hub (or point-to-point)
1000Base-LX	Fiber-optic- two strands of multimode 62.5/125 fiber or monomode fiber	440m (multimode) 5000 m (single mode)	1Gbps	Star, using buffered distributor hub (or point-to-point)
1000Base-CX	Twinax,150-Ohm-balanced, shielded, specialty cable	25m	1Gbps	Star(or point-topoint)
10Base-FL				

IEEE802.11 Wireless

Wi-Fi is the technology used for wireless networking. If your computer has a wireless card, it is most likely Wi-Fi compatible. The wireless card transmits to a wireless router, which is also based on the Wi-Fi standard. Wireless routers are often connected to a network, cable modem, or DSL modem, which provides Internet access to anyone connected to the wireless network.

Wireless –Fidelity (IEEE 802.11) is the standard technology that specifies connectivity for wireless networks. IEEE 802.11, or Wi-Fi, refers to the collective group of standards – 802.11a, 802.11b, 802.11g, and 802.11n. These protocols specify the frequencies, speeds, and other capabilities of the different Wi-Fi standards.

Wireless network standards

Wireless LANs (WLANs) use radio frequencies (RFs) that are radiated into the air from an antenna that creates radio waves.

Because WLANs transmit over radio frequencies, they are regulated by the same types of laws used to govern things like AM/FM radios. It is the Federal Communications Commission (FCC) that regulates the use of wireless LAN devices, and the IEEE takes it from there and creates standards based on what frequencies the FCC releases for public use.

The wireless standards like the Ethernet standards are applied in different situations. The table below clearly describes each type.

Standard	Specification	Advantages	Disadvantages
802.11 Standard	**Rate**: 1Mbps and 2Mbps. It runs in the 2.4GHz radio frequency	-	Slowest.
802.11b Standard	It operates in the 2.4GHz and delivers a maximum data rate of 11Mbps	Lowest cost; signal range is good and not easily blocked	Slowest maximum speed.
802.11g Standard	Bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range.	It is backward compatible with 802.11b.	Costs more than 802.11b.

802.11n standard	It provides up to 300 Mbps of network bandwidth	Best signal range and it is backwardcompatible with 802.11b/g gear.	Standard is not yet finalized; costs more than 802.11g;
802.11ac standard	It operates on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac	It offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz.	-

Table 2. 2: Summary of wireless standards

2.2.3 Range, bandwidth and frequency

One characteristic that measures network performance is bandwidth. The bandwidth reflects the range of frequencies we need. However, the term can be used in two different contexts with two different measuring values: **bandwidth in hertz** and **bandwidth in bits per second**.

a) Bandwidth in Hertz

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

b) Bandwidth in Bits per Seconds

The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit per second. For example, one can say the bandwidth of a Fast Ethernet network is a maximum of 100 Mbps. This means that this network can send 100 Megabits per second.

2.2.3.1 Frequency and Network Range

The higher the frequency of a wireless signal, the shorter its range. 2.4 GHz wireless networks therefore cover a significantly larger range than 5 GHz networks. In particular, signals of 5 GHz frequencies do not penetrate solid objects nearly as well as do 2.4 GHz signals, limiting their reach inside homes.

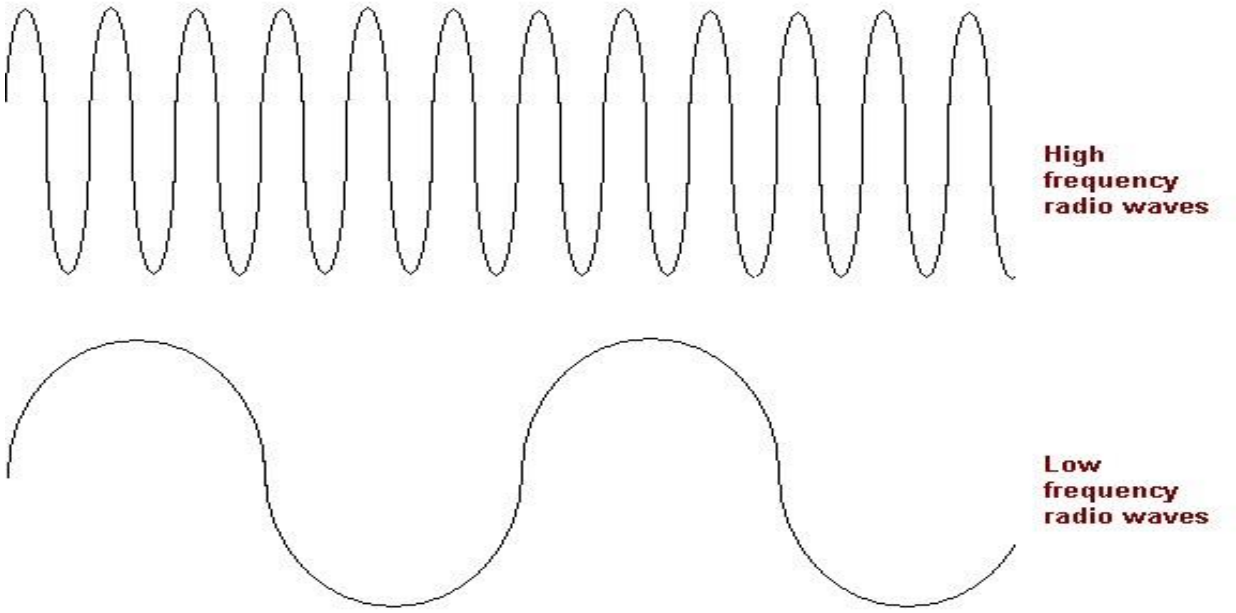
Many older Wi-Fi devices do not contain 5 GHz radios and so must be connected to 2.4 GHz channels in any case.

2.4 GHz	**5 GHz**
802.11b/g/n	802.11a/n/ac
Greater Range (~90 meters)	Lower Indoor Range (~28 meters)
Universal Compatibility	Limited Compatibility (**a**/n/**ac** devices only)
3 non-overlapping channels	24 non-overlapping channels
Congested with Wi-Fi	Little Wi-Fi congestion
Plagued by non-Wi-Fi interference	Very little non-Wi-Fi interference

Table 2. 3: 2.4 and 5 GHz Comparison

2.2.3.2 Range, Bandwidth and Frequency

-The term ‘Bandwidth’ refers to the speed at which data is transferred over the wireless network (more bandwidth means faster downloading and uploading)
- The term ‘Range’ refers to the maximum distance from the router at which the network can be received (the greater the range, the further you can be from the router and still be connected). - The term ‘Frequency’ refers to the number of waves that pass a fixed place in a given amount of time. So if the time it takes for a wave to pass is is 1/2 second, the frequency is 2 per second. If it takes 1/100 of an hour, the frequency is 100 per hour.



Usually frequency is measured in the hertz unit, named in honor of the 19th-century German physicist Heinrich Rudolf Hertz. The hertz measurement, abbreviated Hz, is the number of waves that pass by per second. For example, an **"A"** note on a violin string vibrates at about 440 Hz (440 vibrations per second).

2.2.3.3 Advantages and Disadvantages of the 2.4 GHz and the 5 GHz Wireless Networks

2.4 GHz Wireless Networks		5 GHz Wireless Networks	
Advantages	Disadvantages	Advantages	Disadvantages
It is cheaper to manufacture devices that use this frequency. As a result, this frequency has	• It has a lower bandwidth than the 5 GHz network. • Devices such as cordless phones	• It has a much higher bandwidth than the 2.4 GHz network. • This network is not used by common	It is more expensive to manufacture devices that use this frequency, therefore, only few wireless

become standard and all Wi-Fi enabled devices can use this network. □ It has a much better range than a 5 GHz wireless network. This is due to the fact that the radio waves are able to penetrate solid objects (such as walls and floors) much better than the 5 GHz radio waves.	and microwaves use the same 2.4 GHz radio waves as a wireless router. If you have such devices at home, they can cause interference with the radio waves from the router, causing the network's bandwidth to be reduced. □ More devices support this frequency so there is more congestion in this frequency which may cause issues with bandwidth.	wireless devices such as cordless phones; therefore, there will be no or very little interference to cause a reduction in bandwidth.	devices can use this network. • It has a much lower range than the 2.4 GHz wireless network. Being the higher frequency of the two, it is not able to penetrate solid objects as great as the 2.4 GHz radio waves. • As this is a newer standard and more expensive to implement, fewer devices support this frequency • s this is a newer analyzed the pros and the cons for both the 2.4 GHz and the 5 GHz wireless networks, which wireless network do you think will be the best for you?

2.2.3.4 Token ring

Token ring or IEEE 802.5 is a network where all computers are connected in a circular fashion. The term token is used to describe a segment of information that is sent through that circle. When a computer on the network can decode that token, it receives data.

A Multistation Access Unit (MSAU) is a hub or concentrator that connects a group of computers ("nodes" in network terminology) to a token ring local area network. For example, eight computers might be connected to an MSAU in one office and that MSAU would be connected to an MSAU in another office that served eight other computers. In turn, that MSAU could be connected to another MSAU in another office, which would be connected back to the first MSAU. Such a physical configuration is called a star topology. However, the logical configuration is a ring topology because every message passes through every computer one at a time, each passing it on to the next in a continuing circle.

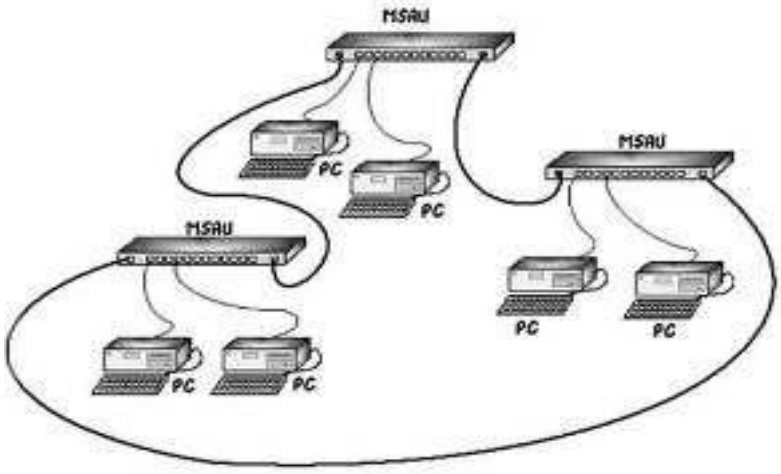


Figure 2. 3: Multistation access unit (MSAU)

Learning Outcome 1.2: Describe Network topology

Definition of topology

- Network topology types

Logical

Physical

- Advantages and disadvantages of topology

3.9. Network Topology

ACTIVITY 3. 11

Draw a Peer -to-peer network and assign each host an IP address.

Instruction :

Network must have 1 switch, 8 computers, one printer which has NIC card and a printer .

The network topology describes the configuration of network, the physical and logical arrangement of nodes that form a network.

costs considerations for choosing a topology

The following factors should be considered when choosing a topology:

- Installation
- Maintenance and troubleshooting
- Expected growth
- Distances
- Infrastructure
- Existing network

As a general rule, a bus topology is the cheapest to install, but may be more expensive to maintain because it does not provide for redundancy.

Network topologies are classified as physical, logical and signals topologies.

Physical topology describes the mapping of network nodes and physical connection between them.

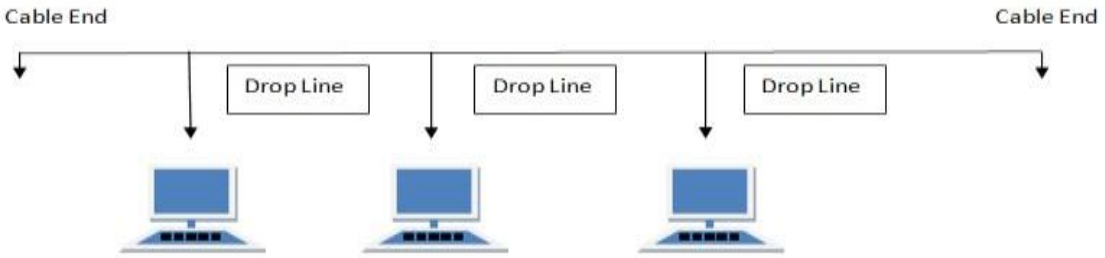
Signal topology describes the paths which signals take while they pass over network that mapping of the paths taken by data as they travel over network.

A **logical topology** is the way data signals pass from one device to another.
There exist different types of network topologies which are Bus topology, Ring topology, Star topology, Mesh topology, Tree topology and Hybrid topology,

3.9.1 BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

It is the most used and employed in LAN architecture. All devices are connected to a central cable, called the bus or backbone. This topology is relatively inexpensive and easy to install for small networks.



Picture 3. 30: BUS Topology

Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

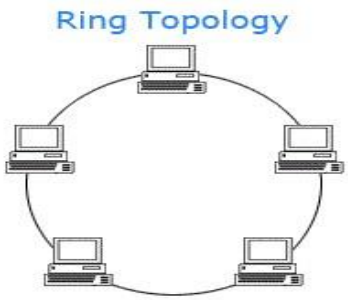
Table 3.3: *advantages and disadvantages of Bus topology*

Advantages of Bus Topology	**Disadvantages of Bus Topology**
1. It is cost effective. 2. Cable required is least compared to other network topology. 3. Used in small networks. 4. It is easy to understand. 5. Easy to expand joining two cables together.	1. Cables fails then whole network fails. 2. If network traffic is heavy or nodes are more the performance of the network decreases. 3. Cable has a limited length. 4. It is slower than the ring topology.

3.9.2 RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

In a Ring topology each device is connected directly to two other devices, one on either side of it, to form a closed loop. This topology is relatively expensive and difficult to install, but it offers high bandwidth and can span large distances



Picture 3. 31: Ring Topology

A ring topology is a computer network configuration in which computer connections create a circular data path. Each networked computer is connected to two others like points on a circle. In a ring network, data travel from one device to the next until they reach their destination. Most ring topologies allow data to travel only in one direction called a unidirectional ring network.

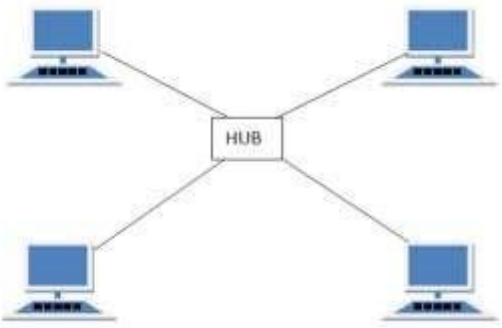
Others permit data to move in both directions called bidirectional.

Table 3.4: *advantages and disadvantages of Ring topology*

Advantages of Ring Topology	**Disadvantages of Ring Topology**
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data. 2. Cheap to install and expand	1. Troubleshooting is difficult in ring topology. 2. Adding or removing the computers disturbs the network activity. 3. Failure of one computer disturbs the whole network.

3.9.3 STAR Topology

In this type of topology all the computers are connected to a single hub or a switch through a cable. This hub or switch acts as the central device and all others nodes are connected to the central device.



Picture 3. 32: Star Topology

So, in a Star topology all devices are connected directly to a central computer or server. Such networks are relatively easy to install and manage

Features of Star Topology

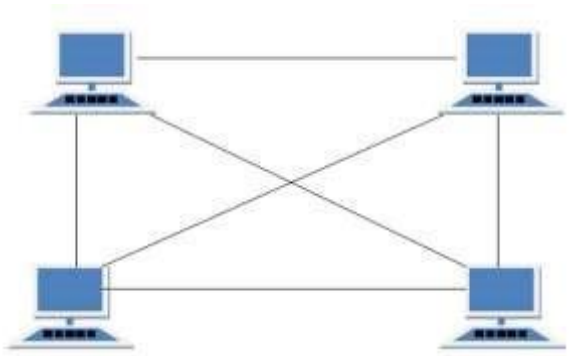
1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair or coaxial cable.

Table 3.5: *advantages and disadvantages of Star topology*

Advantages of Star Topology	**Disadvantages of Star Topology**
1. Fast performance with few nodes and low network traffic. 2. Hub can be upgraded easily. 3. Easy to troubleshoot. 4. Easy to setup and modify 5. Only that node is affected which has failed, rest of the nodes can work smoothly.	1. Cost of installation is high. 2. Expensive to use. 3. If the hub fails then the whole network is stopped because all the nodes depend on the hub. 4. Performance is based on the hub that is it depends on its capacity

3.9.4 MESH Topology

- It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. A Mesh topology can be either a full mesh or a partial mesh. In the former, each computer is connected directly to each of the others.



Picture 3. 33: Mesh Topology

Types of Mesh Topology

1. **Partial Mesh Topology:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

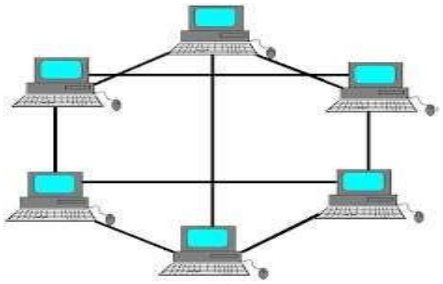


Figure 3.34: Partial mesh topology

2. **Full Mesh Topology:** all devices are connected to each other which is very expensive but provides the best redundancy as a failure of a single does not affect the network connectivity.

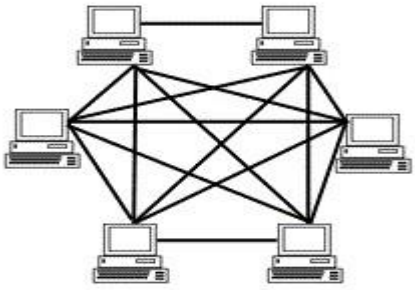


Figure 3.35: Full mesh topology

Features of Mesh Topology

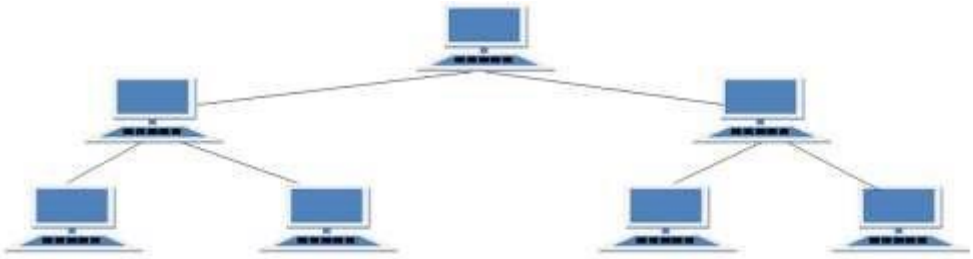
1. Fully connected.
2. Robust.
3. Not flexible.

Table 3.6: *advantages and disadvantages of Mesh topology*

Advantages of Mesh Topology	**Disadvantages of Mesh Topology**
1. Each connection can carry its own data load. 2. It is robust. 3. Fault is diagnosed easily. 4. Provides security and privacy.	1. Installation and configuration is difficult. 2. Cabling cost is more. Bulk wiring is required

3.9.5 Tree Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels of hierarchy.



Picture 3. 36: Tree Topology

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Table 3.7: *advantages and disadvantages of Tree topology*

Advantages of Tree Topology	**Disadvantages of Tree Topology**
1. Extension of bus and star topologies. 2. Expansion of nodes is possible and easy. 3. Easily managed and maintained. 4. Error detection is easily done.	1. Heavily cabled. 2. Costly. 3. If more nodes are added maintenance is difficult. 4. Central hub fails, network fails.

3.9.6 Hybrid Topology

Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology that integrate two or more different topologies to form a resultant topology which has good points (as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

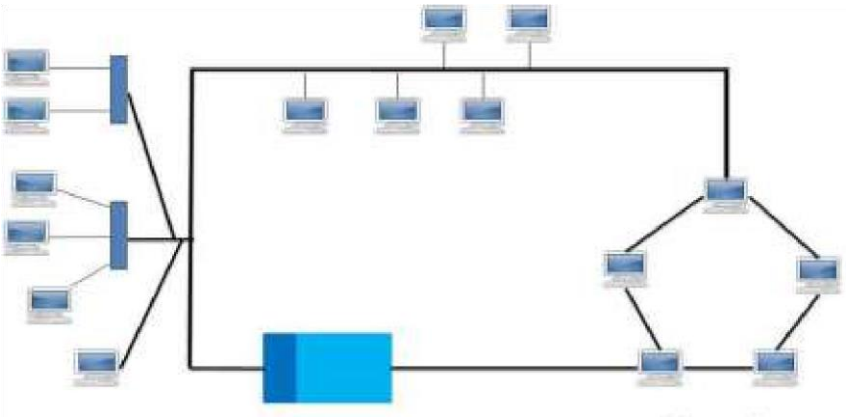


Figure 3.37: Full mesh topology

For example, if there exists a ring topology in one office department while there is a bus topology in another department, connecting these two will result in hybrid topology. However, connecting two similar topologies cannot be termed as Hybrid topology.

Table 3.8: *advantages and disadvantages of Hybrid topology*

Advantages of hybrid Topology	**Disadvantages of hybrid Topology**
1. **Reliable:** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. 2. **Scalable:** It's easy to increase the size of network by adding new components, without disturbing existing architecture. 3. **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. 4. **Effective:** Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized.	1. **Complexity of Design:** One of the biggest drawbacks of hybrid topology is its design. 2. **Costly Infrastructure:** As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticate network devices, etc.

Notice that the cost of technology, network devices, and transmission mediums to be used in the computer network has to be considered while choosing the network topology to use.

APPLICATION ACTIVITY 3.20

1. Using clear example, compare computer network devices, network peripherals and computer peripherals?

2. In an organization there are 20 computers distributed into different offices and all offices share one printer .The managements wants to build a computer network that connects all the computers and printer.

i. Identify a topology to use in this situation

ii. Draw arrangement of computers using identified topology

END OF UNIT ASSESSMENT ACTIVITY

1. Perform the following activity to monitor the internet connection

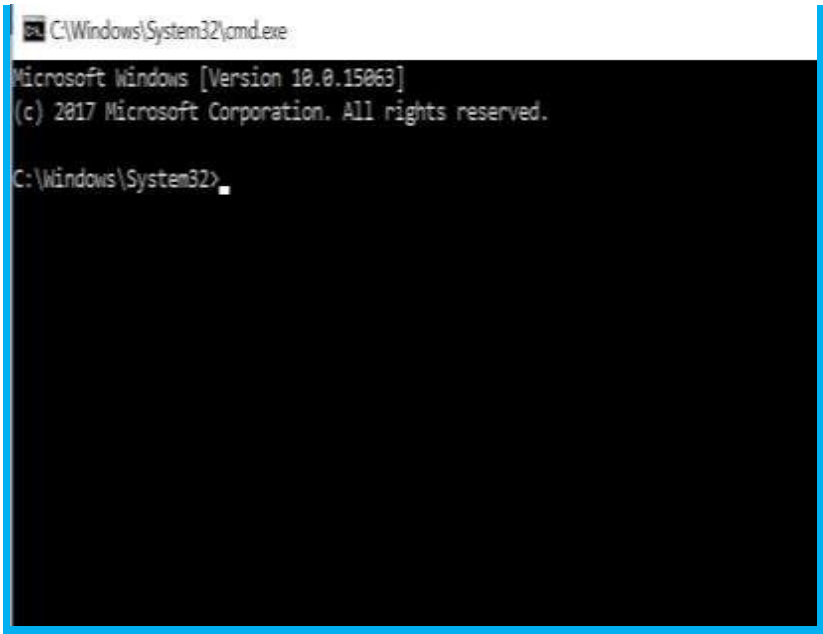
Step1: Search for Command Prompt windows 10

Click start -> search box in windows 10

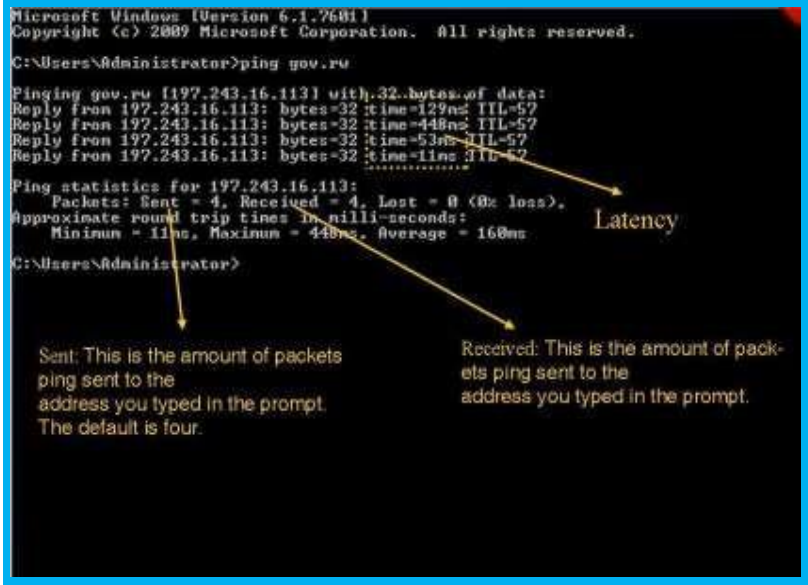
Type CMD

A window will appear with a black screen similar to the one below

Step 2: Welcome Command Prompt Screen



Step 3: Ping a host : ping gov.rw



Step 4: Understanding the Results

Ping Statistics:

Sent: This is the amount of packets ping sent to the address yo u typed in the prompt. The default is four.

Received: This is the amount of packets that returned from the address you typed in the prompt. Ideally, this should equal the amount sent.

Lost: This is the amount of packets that did not return from the address you typed. Ideally,

this should be zero.

Approximate Round Trip Times:

Minimum: This is the shortest time (in milliseconds) that it took for a packet to be sent to the address you typed and returned back to your computer. That is the "Round Trip" it is talking about.

Maximum: This is the longest time (in milliseconds) that it took for a packet to be sent to the address you typed and returned back to your computer.

Average: This is the average round trip time of all the packets sent. Ideally, this should be as low as possible. In the picture from the last step, the average was 3ms, which is very good. The larger the number here, the worse your connection is.

2. Define a computer network.
3. Discuss using examples the purpose of computer network in any organization.
4. Discuss advantages and disadvantage of using computer network
5. Using a clear example, differentiate MAC address and IP address
6. Discuss and compare various types of computer networks
7. Discuss different factors that must be considered before making a choice for the network topology.
8. What do you understand by network subnet?
9. Draw a Client-Server network diagram and explain the role of each component of the client server network.
10. What are similarities and difference between bus topology and tree topology
11. With a clear example, differentiate hub and switch in LAN.
12. What do you understand by transmission medium? Discuss various transmission medium used in computer network.

Wireless topology

It requires only base backbone segment to connect the wireless cell to the wired network if there is one. Wireless networks involve transmitting a signal in some manner (microwave, radio waves, laser, infrared) from an access point, which is a transmitting and receiving device (transceiver).

Wireless topology advantages

-Portability: it is easily carried or moved from place to place.

-Can be operated without cable(phones)

-Can be operated in moving vehicles(radios)

Wireless topology disadvantages

Slow due to emerging technology

Unreliable due to bad weather, range, misalignment, or line-of-sight issues (the state of the atmosphere with regard to temperature, cloudiness, rainfall, wind, and other meteorological conditions) Relatively expensive, although prices are decreasing as it becomes more popular

Learning Outcome 1.3: Study network devices, components and their functions

Network devices classification

Interconnection devices

Access devices

End devices

- Network components

Media

Message

Protocol

Devices

Router

Hubs

Switch

NIC

Repeater

MAU

Firewall

Access points

Antenna

Gateways

Physical Components

Definition of network device

A network host or a node is a computer or any other device that is directly connected to a computer network. A network host may offer information resources, services, and applications to users.

i. Network Interface Card (NIC)

Picture 3. 11: Network Interface Card

Network Interface card is a component that allows the computer to communicate across a network. This component is frequently built into the motherboard of today's computers, but it can also be a separate card for use in a PCI slot.

A **Network Interface Card** (NIC) is an adapter that usually sits in a slot inside the PC. The network interface card handles the connection to the network itself through one or more connectors on the backplane of the card. You must make sure that the network interface card you are using in your machine works with the network operating system.

Network Interface cards be either wired or wireless.

However, some cards do support both wireless and wired networking

Note: A wireless NIC has an antenna connected to the back of the card or attached with a cable so that it can be positioned for the best signal reception. You must connect and position the antenna.

Picture 3. 12: Wireless Network Interface Card

- Important considerations to bear in mind when selecting a NIC to use on a network:

The type of network – NICs are designed for Ethernet LANs, Token Ring, Fiber Distribute Data Interface (FDDI), and so on. An Ethernet NIC will not work with Token Ring and vice versa.

The type of media –The type of port or connector that the NIC provides determines the specific media types such as twisted-pair, coaxial, fiber-optic, or wireless.

The type of system bus –The type of NIC required on the network may determine the system bus requirement in the device. A PCI slot is faster than ISA (Industry Standard Architecture).

- The network cards translates data from the computers and convert them into signals so as to be transmitted across the transmission medium.
- Data when inside a computer travels in parallel form at 8, 16 or 32 bits at a time. The network card converts these signals coming to it in parallel form into a serial signal that can travel across the transmission medium.
- The mechanism of data conversion is in two forms:

The network cards driver converts the data into a format that can be understood by the network card.

The second part is performed by the physical network card. This is the point at which the actual data is converted into a serial format

- It also accesses the transmission medium and forms a channel to conduct the signal. Onto the network.

*ii.*Media Access Control Address

Media Access Control Address (MAC address) of a device is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC address is a physical address of Network Interface Card. In other words MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter when it is manufactured.

Example of a MAC address: *00:0a:95:9d:68:16.*

iii. **Modem**

A modem is a hardware device that enables a computer to send and receive data over a telephone line or a cable or satellite connection. Modem is used to transmit digital information via analog systems. The word "modem" is derived from the term "**Mo**dulator - **Dem**odulator."

The essential functions of a modem are:

- **Modulate:** an analog carrier signal to carry digital information, it means to convert the analog signal to digital signal.
- **Demodulate**: a similar signal so as to decode the digital information from the analog carrier signal and it means to convert the same signal back to the analog signal then transmitted through telephone line.

They are two types of modem:

Internal modem: Internal modems are circuit boards that plug into a computer's motherboard **External Modem:** An external modem is a discrete unit housed in a separate case. Typically, an external modem is connected to the telephone line and the computer via cables or USB.

Picture 3. 13: Modem s

APPLICATION ACTIVITY 3.8

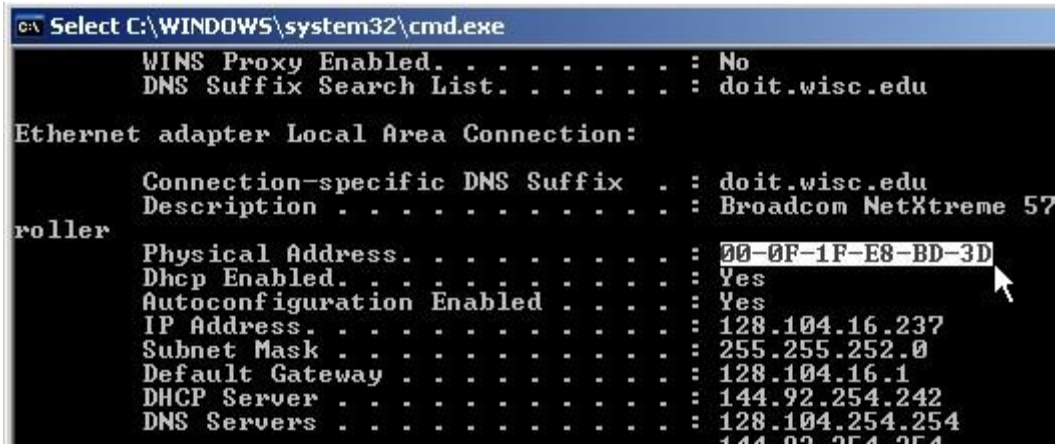
Find the Mac address of your computer

Step1: Click the **Run** button in the windows 10 **Start Menu**

Step 2: Type **cmd** in the **Open** prompt of the Run menu and click **OK** to launch a command prompt window

Step 3: Type **ipconfig /all** at the command prompt to check the network card settings.

Step4: MAC address is listed by ipconfig under **Physical Address**



iv. RJ 45 Connector and Port

A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment. The physical connectors that registered jacks use are mainly of the modular connector and 50-pin miniature ribbon connector types

Picture 3. 14: RJ 45 Connector and Port

The RJ45 port is the network port on a computer. This socket has many names. It is also known as the Ethernet port, the network adapter, the network jack or the RJ45 jack.

Network Devices

1 Hub

A hub is a network hardware device for connecting multiple devices together and making them act as a single **network segment.**

A **Hub** is a multipurpose network device that lies at the center of a star-topology network. Most hubs do the same job as concentrators. Hubs support a variety of different interface cards, from concentrator cards to router cards. Hubs are also expandable within a single

chassis. Despite these differences, the term *hub* and *concentrator* are often used interchangeably. There are active and passive hubs.

Definition:

A **network segment** is a portion of a computer network that is separated from the rest of the network by a network device.

Hub receives message on one port and then send it out to all other ports, this means that when hub receives message, the received message is regenerated or duplicated and sent to all computers connected to the hub, each computer on the network receives the message, if it is not the destination message is destroyed, if it is the destination it reads the message.

Picture 3. 15: HUB

Note: Hub are used less often today because of the effectiveness and low cost of switch. Hub do not segment network traffic. When one device sends traffic, the hub floods that traffic to all other devices connected to hub. The devices are sharing the bandwidth.

Hubs are devices that extend the range of a network by receiving data on one port, and then regenerating the data and sending it out to all other ports. This process means that all traffic from a device connected to the hub is sent to all the other devices connected to the hub every time the hub transmits data. This causes a great amount of network traffic. Hubs are also called concentrators, because they serve as a central connection point for a LAN.

2 **Switches**

Switch filters and segments network traffic by sending messages only to the device to which it is sent. This means that when a switch receives a message do not duplicated it, it sends it directly to the destination computer. This provides higher dedicated bandwidth to each device on the network.

Picture 3. 16 : SWITCH

A switch maintains a switching table, the switching table contains a list of all MAC addresses of computers on the network and a list of switch port which are used to reach a computer with a given MAC address.

When message arrives that is destined for a particular MAC address, the switch uses the switching table to determine which port to use to reach the MAC address. Then message is forwarded to the destination.

An Ethernet switch is a device that provides a central connection point for cables from workstations, servers, and peripherals. Most switches are active, that is they electrically amplify the signal as it moves from one device to another. A switch maintains a table of the MAC addresses for computers that are connected to each port. When a frame arrives at a port, the switch compares the address information in the frame to its MAC address table. The switch then determines which port to use to forward the frame

The features of Switches are:

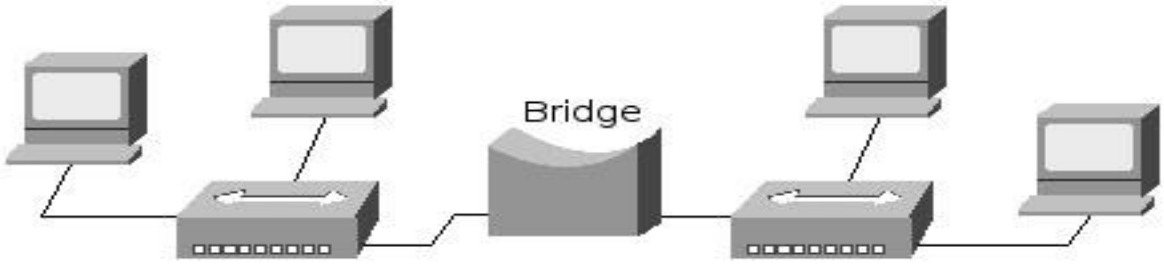
- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or tree topology
- Available as "managed" or "unmanaged", with the later less expensive, but adequate for smaller networks
- Replace the hubs, immediately reducing network traffic in most networks

- Usually installed in a standardized metal rack.

3 Bridge

A **Bridge** is a network device capable of connecting networks that use similar protocols. It connects two local area networks running the same network operating system.

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. This function is called **network bridging**



Picture 3. 17: Two network segments connected via a bridge

Bridges were introduced to divide LANs into segments. Bridges keep a record of all the devices on each segment. A bridge can then filter network traffic between LAN segments. This helps reduce the amount of traffic between devices

A bridge is a device used to filter network traffic between LAN segments. Bridges keep a record of all the devices on each segment to which the bridge is connected. When the bridge receives a frame, the destination address is examined by the bridge to determine if the frame is to be sent to a different segment, or dropped. The bridge also helps to improve the flow of data by keeping frames limited to only the segment to which the frame belongs.

4 Access point

Picture 3. 18: Linksys access point

The Access Point is connected to a switch using UTP cable, therefore it can provide access to the rest of the network. Instead of providing copper cabling to every network host, only the wireless access point is connected to the network with copper cabling and spread radio waves to the rest of network.

The range (radius of coverage) for Access Point indoors is 98.4 ft (30 m) and too much greater distances outdoors depending on the technology used.

APPLICATION ACTIVITY 3.9

1. Justify why outdoor range is better that indoor range?
2. Discuss how a switch perform micro-segmentation?
3. Analysis why Switch is much preferred than a HUB
4. Examine the difference between Access Point and Bridge?
5. Identify the purpose of switching table in the switch?

5. Repeater

A **Repeater** is a network device that increases the power of incoming signals to allow the length of a network to be extended.

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded

twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

6.Router

A **Router** is physical device that join multiple wired or wireless networks together in other words Router is a network device that connects LAN's, that may be running on different operating systems, into an internetwork and routes traffic between them.

Router is device that connects entire network to other networks. Router uses IP addresses to forward frames to other networks. A router can be a computer with special network software installed, or a router can be a device built by network equipment manufacturers. Routers contain tables of IP addresses along with optimal destination routes to other networks.

If you have a school LAN that you want to connect to the Internet, you will need to purchase a router. In this case, the router serves as the forwarder between the information on your LAN and the Internet. It also determines the best route to send the data over the Internet.

Routers and Access points

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point. It is used to provide access to the Internet or a private computer network. Routers operate at the Network layer (Layer 3) of the OSI Model.

The Wireless access points (APs or WAPs) are networking devices that allow wireless Wi-Fi devices to connect to a wired network.

Figure 2.19: Routers

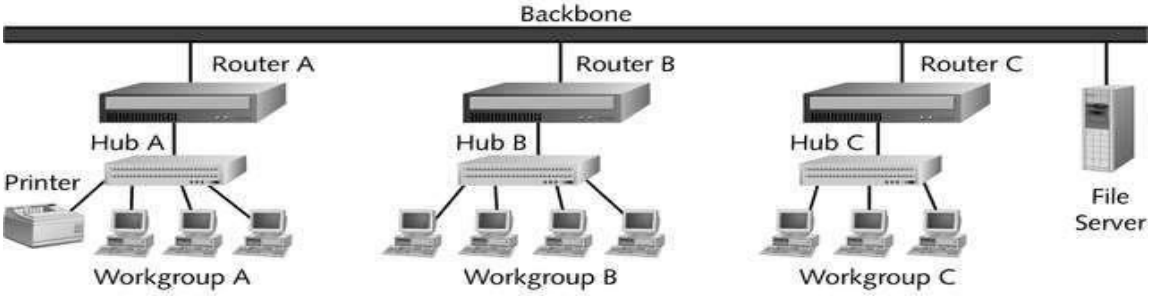


Figure 2.20: The placement of routers in a network

4.3 Configuring a wireless router

Step 1: Get to know your wireless router

- A power input jack one
- One or more wired Ethernet jacks (often labeled 1, 2, 3, 4) for computers on your network which don't have wireless ability.
- One Ethernet jack for your broadband connection, often labeled “WAN” or “Internet.”
- A reset button. to

Step 2: Connect your router a wired PC for initial setup

Figure 2.21: Connecting a wireless router to a PC

Step 3: Open web browser and connect to wireless router administration INTERFACE To connect to your router, you need to know its default IP address and connect your browser to *http://routeripaddress*. For example, if you own a Linksys brand wireless router, its default IP address is **192.168.1.1**, and therefore you open your browser to the URL ***http://192.168.1.1*.** Most wireless routers also require you to log in to access configuration pages. Your router includes a manual or a "quick setup" guide which details both its default IP address and default login.

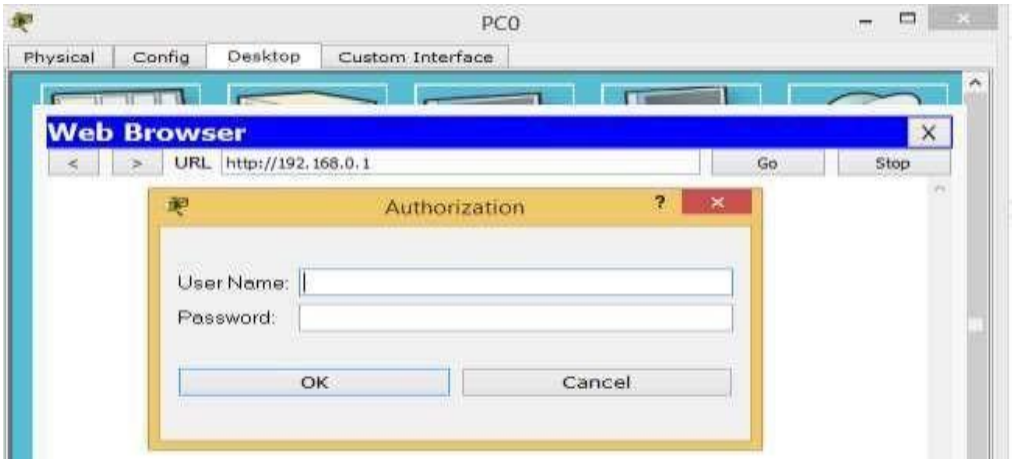


Figure 2.22: Login window

Step 4: Determine your broadband type

There are three common broadband connection methods:

- **DHCP Dynamic IP:** Basic network parameters are automatically assigned to your router by the broadband modem.
- **PPPoE**: Requires you to supply a username and password provided to you by your ISP.
- **Static IP**: Your broadband provider would have supplied you with a set of numeric addresses you need to connect to the network, as they are not assigned automatically.

Figure 2.23: Broadband connection methods

Step 5: Configure your broadband connection

On this model, you clicked the "Setup" menu and "Basic setup" submenu. Again, your model may differ, and newer models may include a guided wizard that takes you through these steps.

Step 6: Configure your wireless network basics

If your router is connected to broadband and it is working successfully, we can setup the wireless networking configuration. On our sample router we clicked the "Wireless" submenu. Assign your wireless network a name, also known as Service Set Identifier *(SSID)*. Choose a unique name in case there may be neighboring wireless routers nearby.

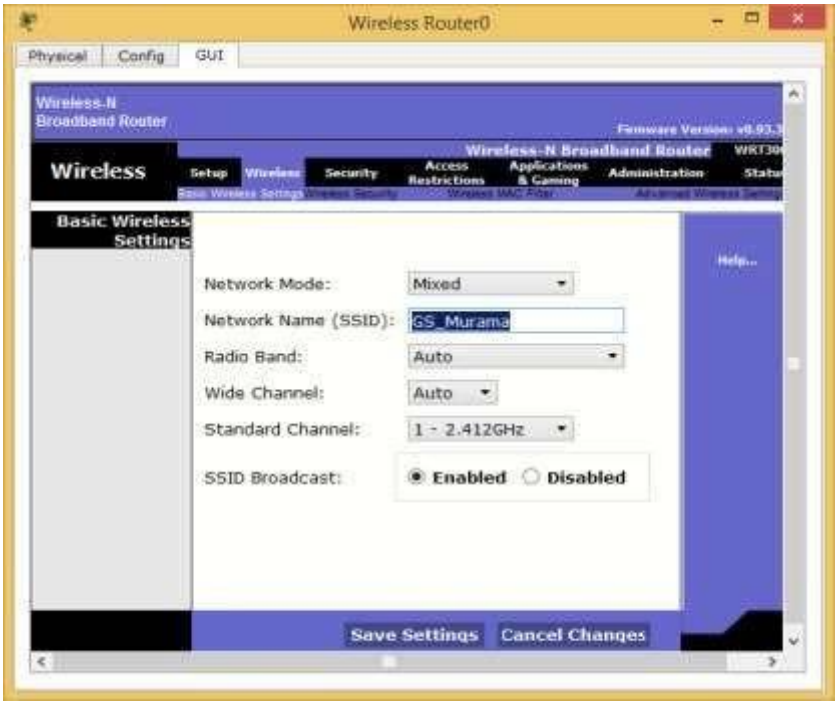


Figure 2.24: Basic wireless settings

Step 7: Configure your wireless security

Most wireless network users will select one of four degrees of encryption security available in wireless hardware today.

Figure 2.25: Encryption security modes

1. WEP: The oldest and least secure data encryption. All wireless gear supports WEP, though, it is useful when you need at least some kind of encryption to be compatible with older wireless hardware.
2. WPA: A more secure upgrade to WEP. Designed so that many older devices which included only WEP can be upgraded to support WPA.
3. WPA2: A significantly more secure upgrade to either WEP or WPA. Cannot upgrade older hardware to WPA2, but many new wireless devices support WPA2.

Note: At each step you must click on the "save Settings" button before you proceed with the next step

2.4.3.1 Router Operation Mode

Many of the routers offers different operation modes that you can use.

a) Wireless Router Mode

In wireless router/ IP sharing mode, the router connects to the Internet via PPPoE, DHCP, PPTP, L2TP, or Static IP and shares the wireless network to LAN clients or devices. Select this mode if you are a first-time user or you are not currently using any wired/wireless routers.

b) Repeater Mode

In Repeater mode, your router wirelessly connects to an existing wireless network to extend the wireless coverage. You will generally use repeaters or wireless extenders when you have hard to reach places with your home Wi-Fi setup.

c) Access Point (AP) Mode

In Access Point (AP) mode, the router connects to a wireless router through an Ethernet cable to extend the wireless signal coverage to other network clients. This mode is best to be used in an office, hotel, and places where you only have wired network.

d) Media Bridge or Client Mode

With client mode or media bridge, it can connect to a wired device and works as a wireless adapter to receive wireless signal from your wireless network. The reason for this mode is that it can increase the speed of your wireless connection so that it matches the speed of the Ethernet connection.

2.4.3.2 Default gateway

A default gateway is used to allow devices in one network to communicate with devices in another network. If your computer, for example, is requesting an Internet webpage, the request first runs through your default gateway before exiting the local network to reach the Internet. The gateway is the address we assigned to the Ethernet port that the desktop is connected to. An easier way to understand a default gateway might be to think of it as an intermediate device between the local network and the Internet.

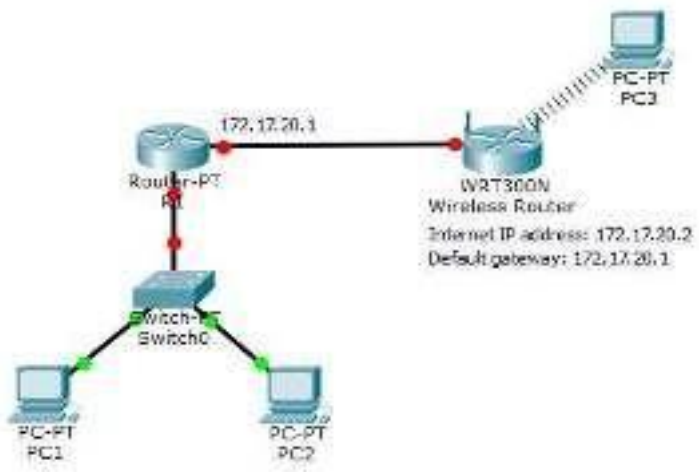


Figure 2.26: Default gateway

a) Configuring the default gateway on a wireless router Start packet tracer, add a wireless router and do the following:

- Click on wireless router and go to GUI tab.
- Set the Internet Connection type to Static IP.
- Configure the IP addressing according to the figure below.
- Scroll down and click on Save Settings.

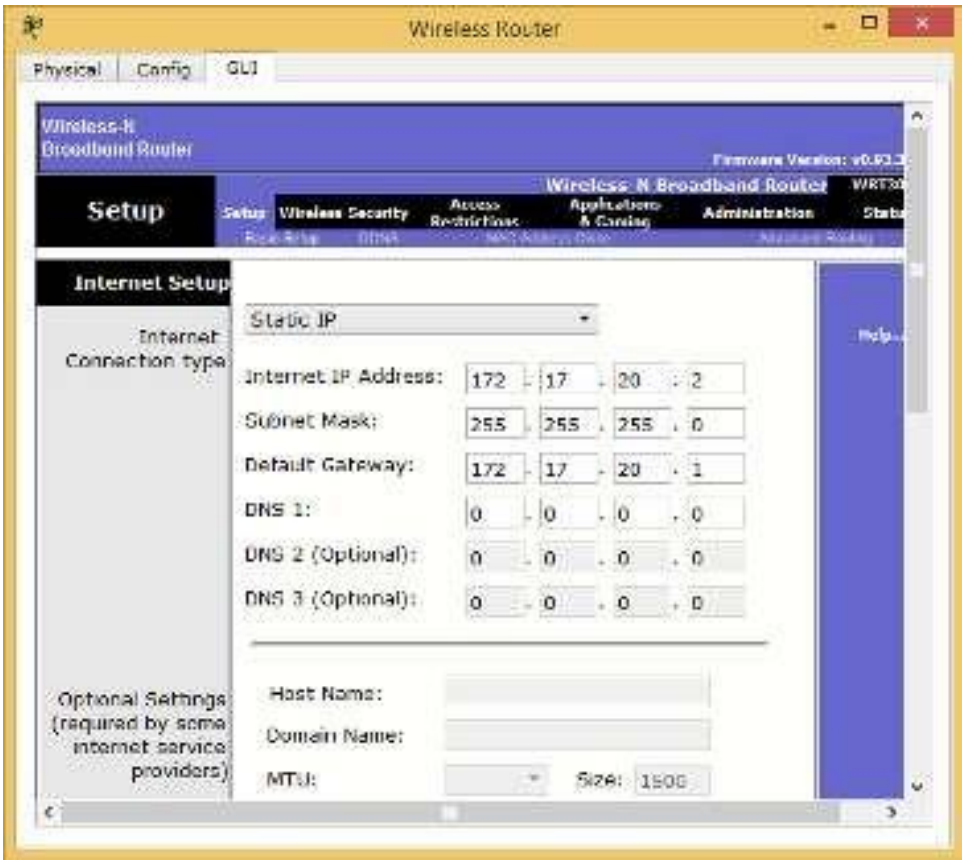


Figure 2.27: Default gateway configuration

b) How to find your default gateway IP address

You might need to know the IP address of the default gateway if there is a network problem or if you need to make changes to your router.

- In Microsoft Windows, the IP address of a computer's default gateway can be accessed through **Command Prompt** with the **ipconfig** command, as well as through the **Control Panel.**
- The ***netstat*** and ***ip route*** commands are used on macOS and Linux for finding the default gateway address.

Figure 2.28: The command prompt window

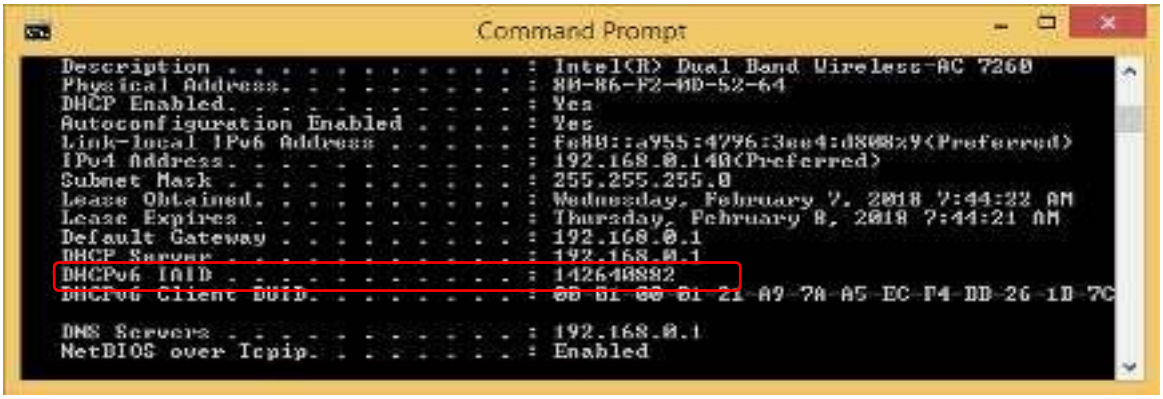


Figure 2. 29: Default gateway

c) Configuring a default gateway on a desktop

- Open the control panel
- Click on Network and Internet
- Click on Network and sharing center
- Click on adapter settings

Figure 2.30: Network and sharing center

- Right click on wi-fi and choose properties

Figure 2.31: Wi-Fi properties 1

- Choose Internet Protocol Version 4 (TCP/IPv4) and click on properties

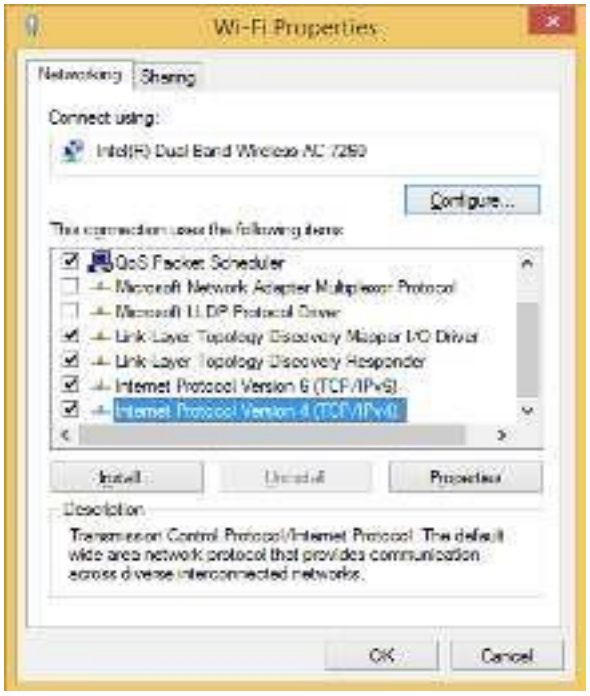


Figure 2.32: Wi-Fi properties 2

- Enter IP address as follows and then click on OK:

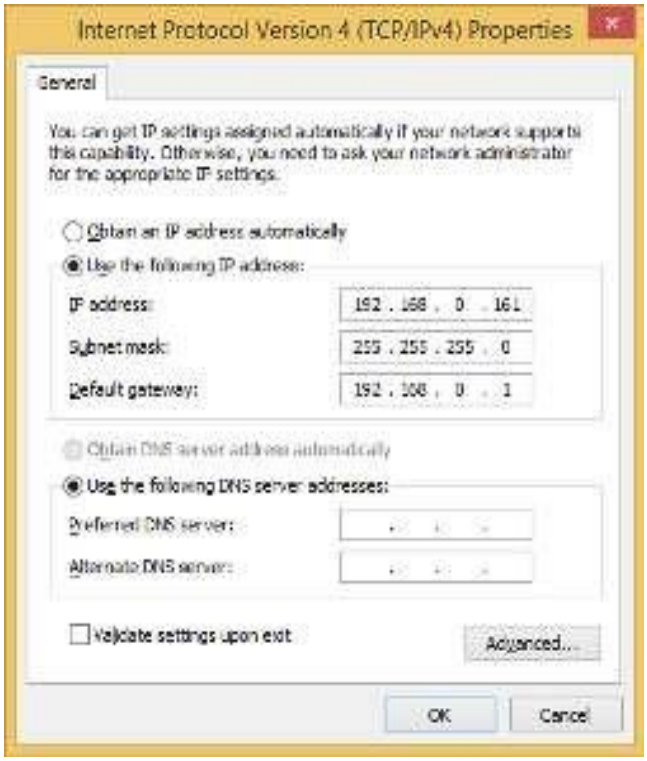


Figure 2.33: TCP/IP properties

2.4.4 Public and private IP

2.4.4.1 Public IP addresses

A public IP address is the one that your ISP (Internet Service Provider) provides to identify your home network to the outside world. It is an IP address that is unique throughout the entire Internet. A public IP address is worldwide unique, and can only be assigned to a unique device

Depending on your service, you might have an IP address that never changes (a fixed or static IP address). But most ISPs provide an IP address that can change from time to time (a dynamic IP address)

Example: Web and email servers directly accessible from the Internet use public IP addresses.

1.4.4.2 Private IP addresses

A private IP address provides unique identification for devices that are within your Local Area Network, such as your computer, your smartphones, and so on. If every device on every network had to have real routable public IP addresses, we would have run out of IP addresses to hand out years ago. Private IP addresses are used for the following reasons:

- To create addresses that cannot be routed through the public Internet
- To conserve public addresses

Examples:

- Computers, tablets and smartphones within an organization are usually assigned private IP addresses.
- A network printer residing in your school computer lab is assigned a private address so that only users within computer lab can print to your local printer.

Notice that IP addresses, public or private, are assigned to devices according to network classes. The most used classes are A, B and C. They differ according to the number of networks and hence to the number of IP addresses in one network. From A to C, the number of possible networks increase while number of available IP addresses in a network reduces.

Address Class	**Reserved Address Space**
Class A	10.0.0.0 through 10.255.255.255
Class B	172.16.0.0 through 172.31.255.255
Class C	192.168.0.0 through 192.168.255.255

Table 2. 4: Reserved IP Address Space

2.4.5 Configuring a wireless Access Point

The physical setup for a wireless access point is pretty simple: you take it out of the box, put it on a shelf or on top of a bookcase near a network jack and a power outlet, plug in the power cable, and plug in the network cable.

To get to the configuration page for the access point, you need to know the access point's IP address. Then, you just type that address into the address bar of a browser from any computer on the network.

For example to configure TP-Link TL-WA701ND Access Point you will follow the following steps:

Step 1: Power the TP-Link TL-WA701ND using the barrel jack or PoE (Power-over-Ethernet) injector, and connect a computer to the access point using an Ethernet cable (if using the PoE injector, connect the LAN port to your computer, and the POE port to the access point).

Step 2: Ensure all wireless interfaces are disabled on the computer (such as WiFi and Bluetooth) and that DHCP is enabled on the Ethernet interface. Open a web browser and access the TLWA701ND by entering 192.168.0.254 into the address bar.

Figure 2.34: Entering Access Point default IP address

Step 3: Log in using username admin and password admin

Figure 2.35: Log in through the browser

Step 4: The Quick Setup wizard will load in the browser. Click Next to start the configuration process.

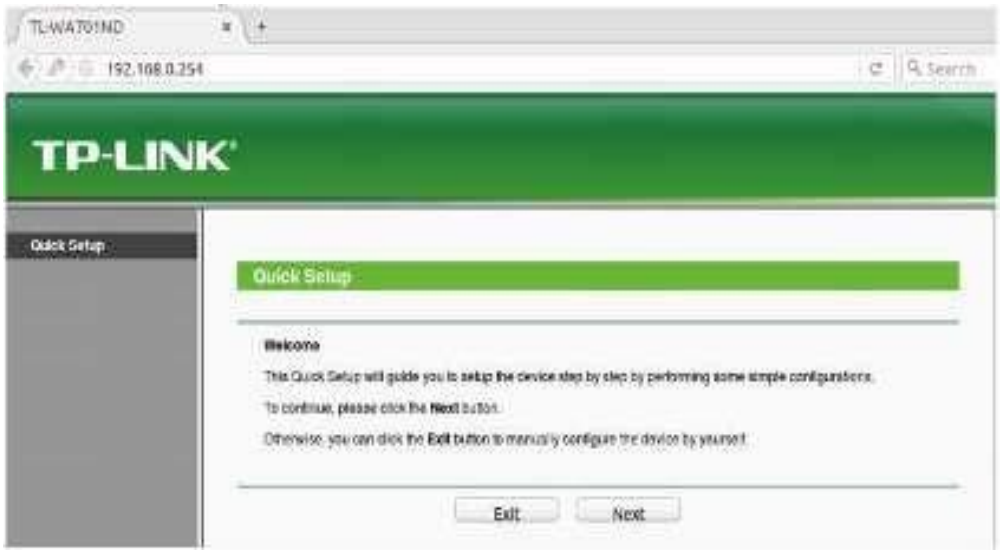


Figure 2.36: Quick setup window

Step 5: Select Client from the list of operating modes. Click Next.

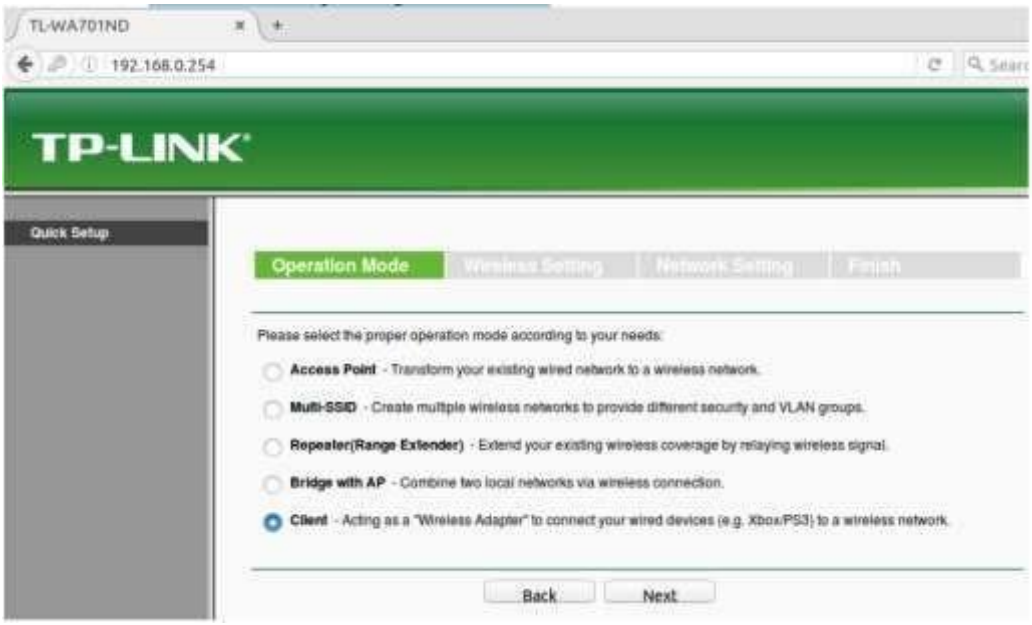


Figure 2.37: Operation mode

Step 6: Click Survey to scan for a list of available wireless access points. Alternatively, skip to step 8 and manually enter information.

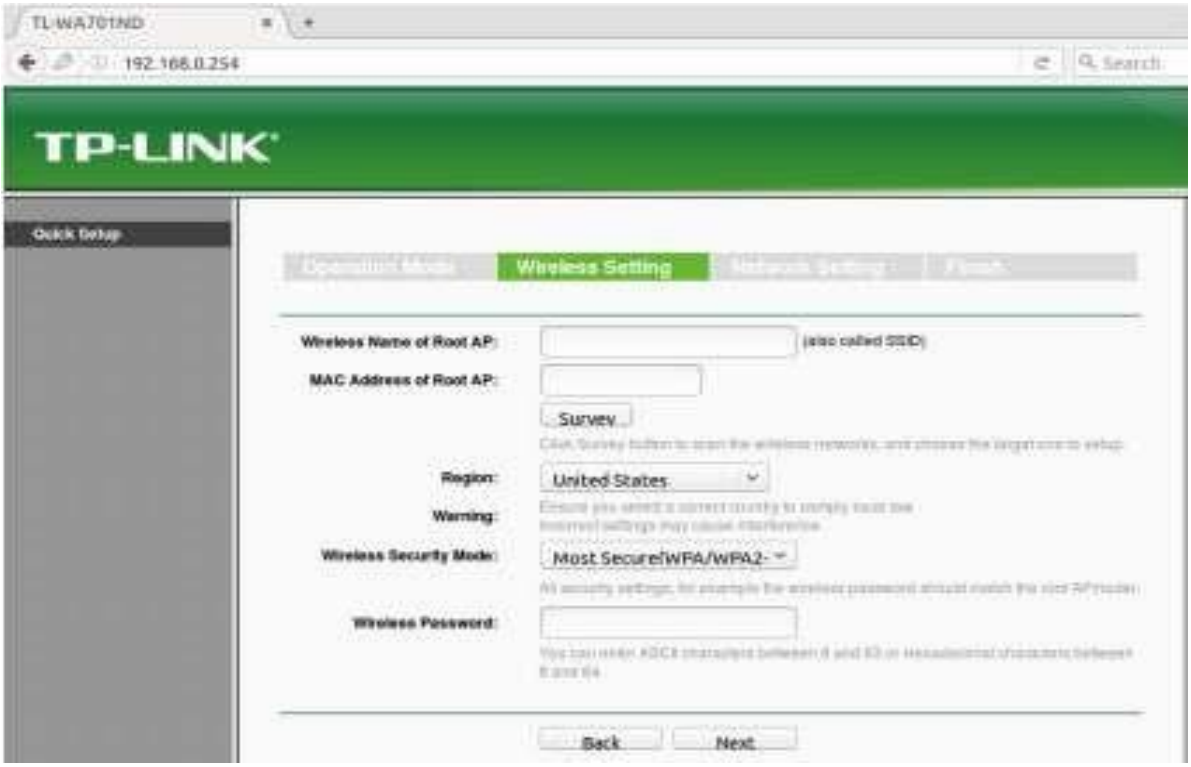


Figure 2.38: Wireless settings

Step 7: From the list of available WiFi networks, select the network to use by clicking Connect to the far right. Make sure the network has a good connection by checking the signal strength. The higher the number, the stronger the connection.

Figure 2.39: Existing wireless

Step 8: Once the Connect option is clicked, these fields will automatically fill in. Alternatively, enter the Wireless Name (SSID) and Wireless Security Mode and Wireless Password. The wireless security settings will need to be manually entered for any password protected WiFi network. Click Next.

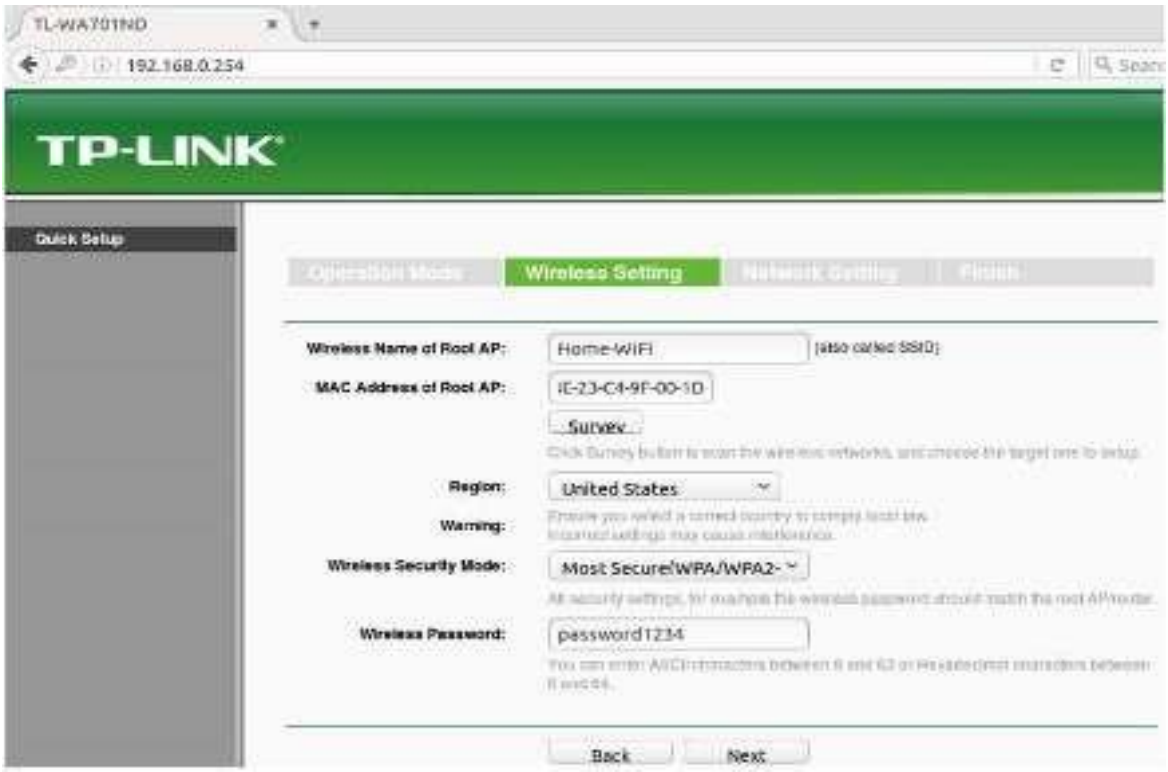


Figure 2.40: Setting wireless name

Step 9: The default values are typically fine for these settings. If needed, obtain the correct settings from the network administrator. Be sure to make a note/take a screenshot of the IP address set in

this step, as it will replace the original fallback IP address. When the correct settings have been applied, click Next.

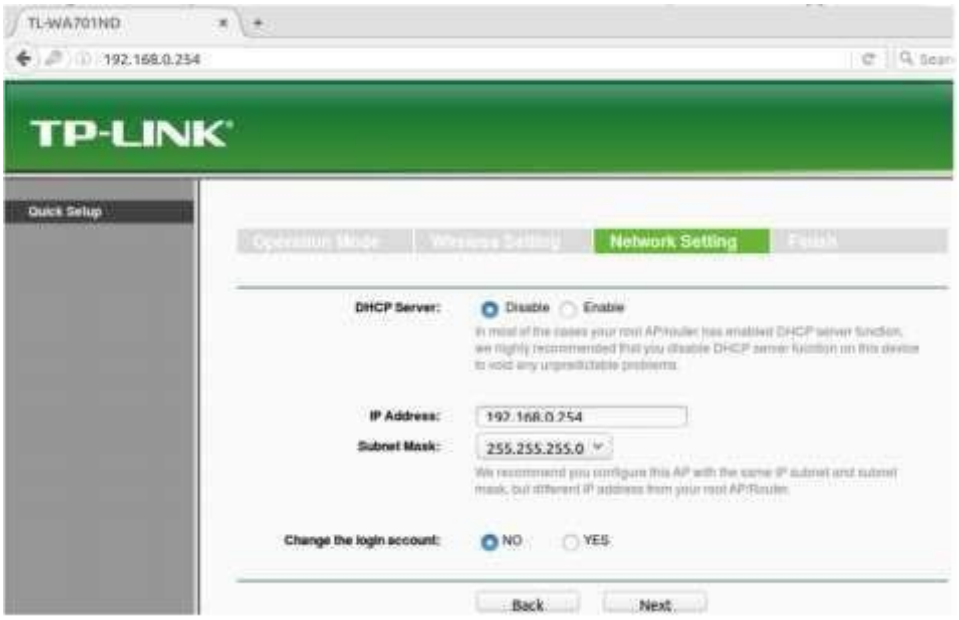


Figure 2.41: Network settings

Step 10: Make a note or take a screenshot of the applied settings if desired, then click Save.

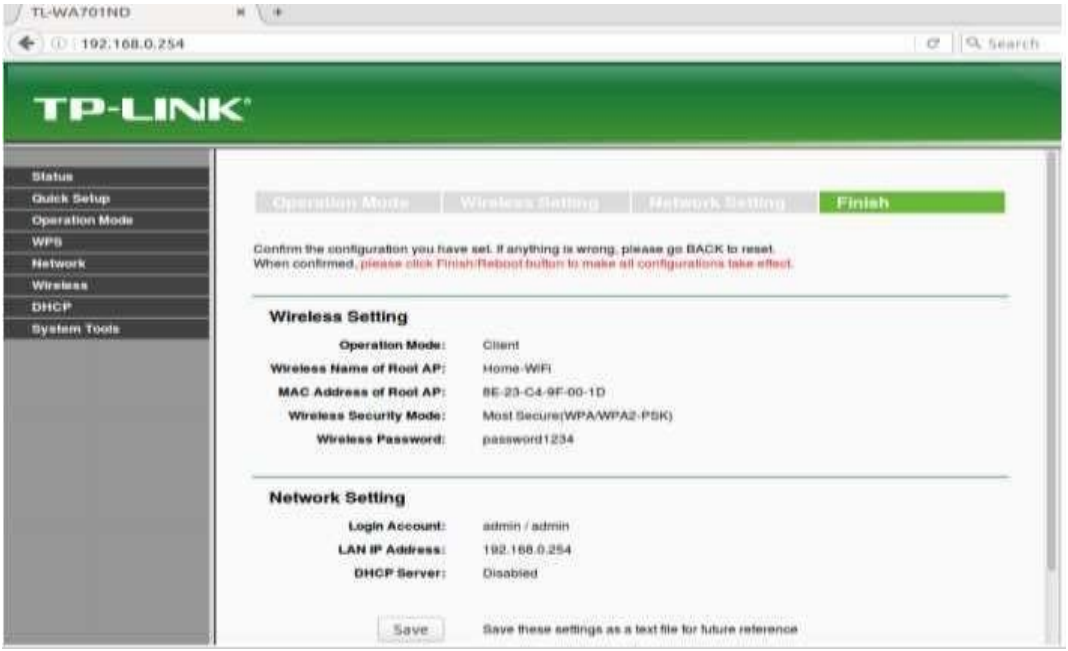


Figure 2.42: Summary of configuration

Step 11: The device will reboot. The configuration page will likely not load; try loading a webpage (e.g. http://www.irembo.gov.rw) while the TP-Link Access Point is connected to the computer to see if there is Internet connectivity.

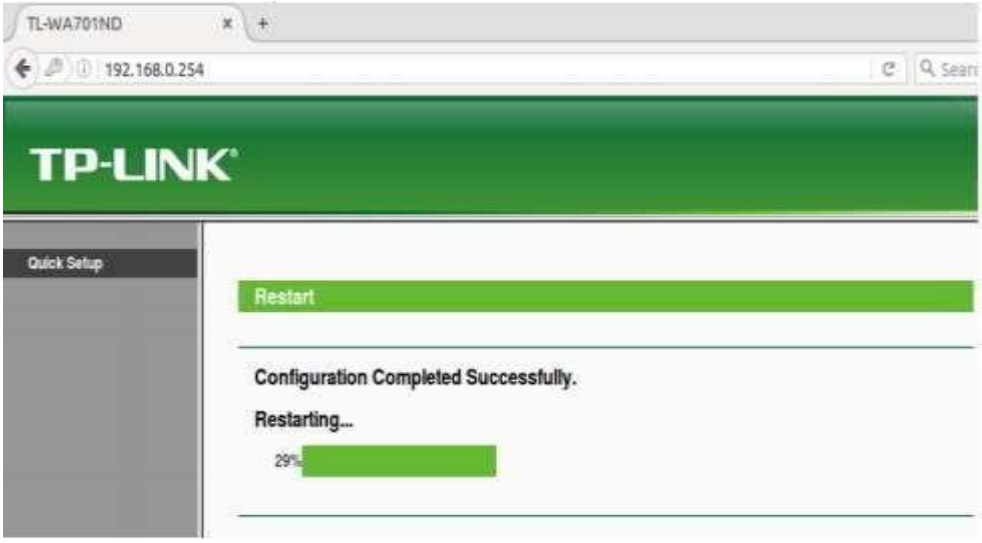


Figure 2.43: Access Point reboot

Step 12: Troubleshooting

- The TP-Link TP-WA701ND does not have any LEDs illuminated
  - Ensure the access point has power either directly to the barrel jack on the back, or via the POE injector's POE Ethernet port. The POE injector requires power via barrel jack.
  - Verify the ON/OFF button next to the access point's Ethernet port is depressed in the ON position.
- I cannot access the device configuration page.
  - The TP-Link WA701ND has a default fallback IP address of 192.168.0.254. To access the device configuration pages, connect a computer directly via an Ethernet cable, configure the computer to use an IPv4 address in the same range (for example, 192.168.0.100), open a web browser, and enter the fallback IP address of 192.168.0.254 in the address bar. If you changed the IP address on the Network Setting page during configuration step 9, use that IP address instead.
- I cannot access the device at all (lost credentials, major configuration issue, etc)
  - The TP-Link TL-WA701ND has a recessed reset button located on the back of the device. This button is closest to the antenna, and a pin or paperclip is needed to press it. Hold the button down for 8+ seconds. All of the LEDs should turn off and back on; after this the initial configuration steps can be used to gain access. Note that this will reset all device settings to the factory default.

2.4.6 How to connect to the Internet through your wireless access point?

a) Connecting to Internet through the control panel

- Open the windows control panel, and then click network and Internet.
- The Network and Internet window appears.

Figure 2.44: The Network and Internet window

- Click network and sharing center.
- The Network and Sharing Center window appears.

Figure 2.45: The Network and Sharing Center window

- Click set up a new connection or network.

Figure 2.46: Set up a new connection of network

- Set up a Connection or Network window appears.
- Click Manually connect to a wireless network

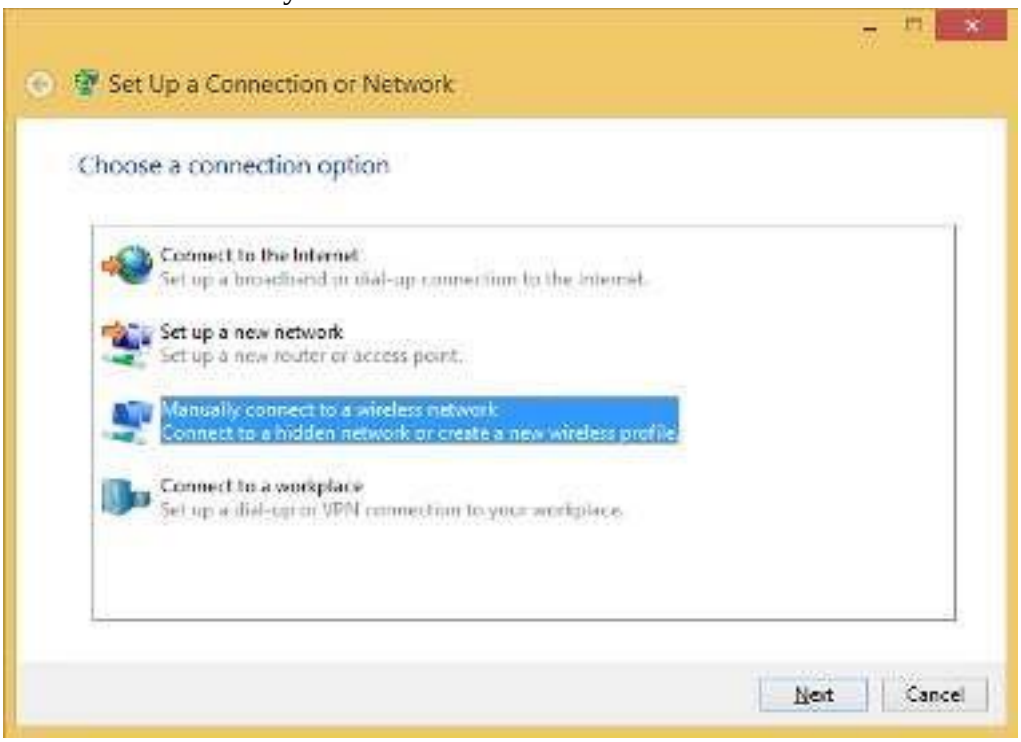


Figure 2.47: Manually connect to a wireless network window

- Click Manually connect to a wireless network

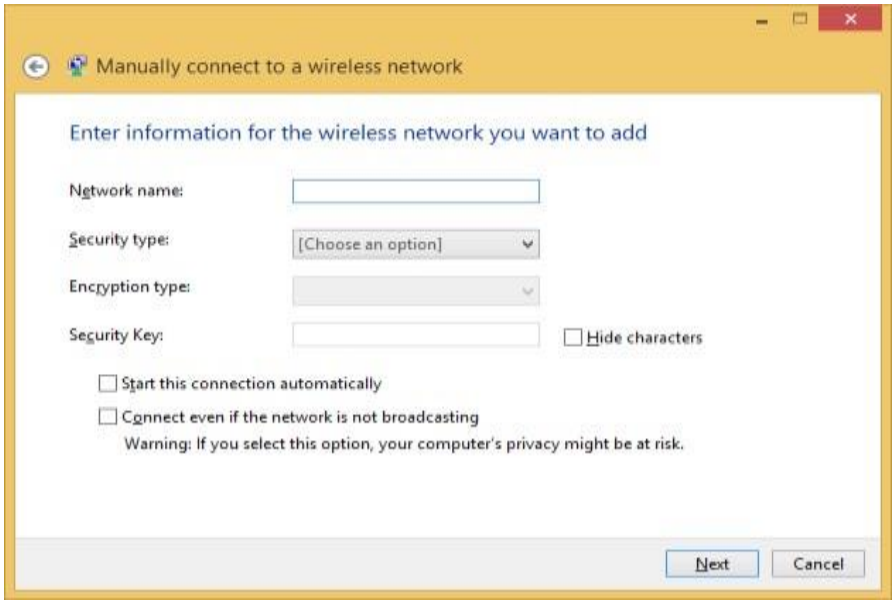


Figure 2.48: Wireless information entry form

- Enter your wireless name in the Network name textbox, for example in our case we want to connect to "**WirelessAP**"
- Choose WPA2-Personal for security type
- Choose AES for encryption type
- Type wireless key in the security key textbox
- Click next

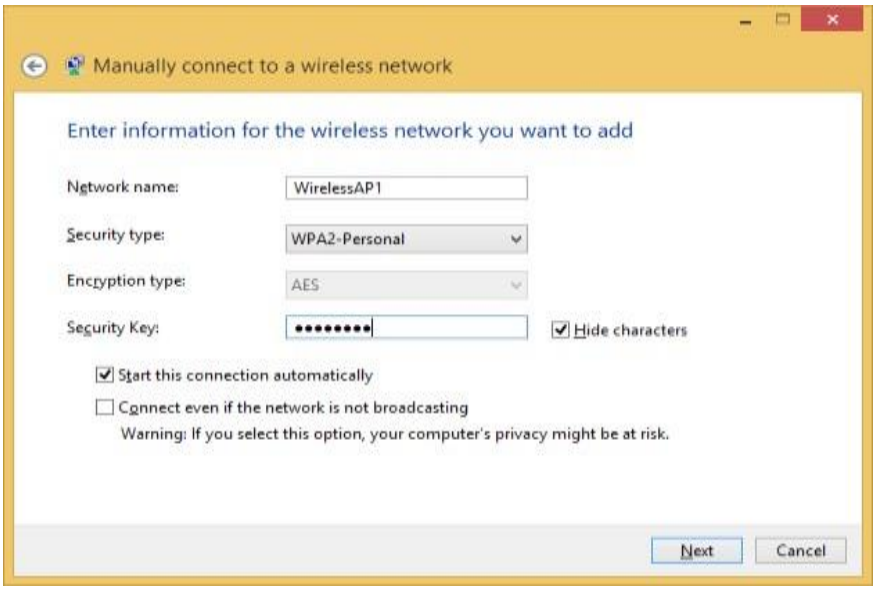


Figure 2. 49: Wireless information captured

- Click next
- Click close

Figure 2.50: Wireless successful message

b) Connecting to the Internet through the Taskbar

1. Select the Network icon in the notification area.

Figure 2.51: Wireless notification icon

2. In the list of networks, choose the network that you want to connect to, and then select Connect.
3. Type the security key (often called the password).
4. Follow additional instructions if there are any.

2.4.7 Wireless Access Point vs Router

The Wireless Access Points (AP) and routers play the similar role but they have some differences. They all connect different networks. *A router often has an Access Point built-in, but a standalone Access Point can't be a router.* An AP can be compared to a modem which is limited in its functionality on managing multiple devices or controlling an entire network with many devices. Routers on the other hand can manage an entire home or small business giving network capability to many computers and devices simultaneously.

2.4.7.1 Wireless Access Point Functions

APs give wireless network ability to any device that only has a hard-wired connection. It is done by plugging in an Ethernet cable and the AP would then communicate with WiFi devices and giving them network access. .

For example a printer that has no built-in wireless can have a access point added which will give it wireless ability.

While current routers have built-in WiFi and play many roles including being an AP, many don't use dedicated AP.APs are still used in many networks and they are used to help with WiFi dead spots and extending a wireless network.

An AP can be added in locations that have bad wireless network ability and give good coverage throughout a home or business.

2.4.7.2 Router Functions

From the above section, a router is a network device that can transfer data wirelessly or wired. It forwards data packets to the desired device and control LAN (local Area Networks) or WAN (Wide Area Networks) networks

Why routers and switches do not operate at the same OSI reference model layer? Answer: Routers (layer 3 devices) use logical addressing and provide what is called packet switching. Routers use a routing table (map of the internetwork) to make path selections and to forward packets to remote networks. On the other side, switches (layer 2 devices) are not used to create internetworks because they do not break up broadcast domains by default; they are employed to add functionality to a network LAN. The main purpose of switches is to make a LAN work well and do not forward packets to other networks as routers do

2.4.7 SSID and encryption

2.4.7.1 SSID and Wireless Networking

An SSID (Service Set Identifier) is the primary name associated with an 802.11 Wireless Local Area Network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks.

When you right click on the icon of wireless network in the Task Bar (Bottom Right of the computer's screen), the displayed list of names of different networks are the SSID that are covered now or have been used in past.

On home Wi-Fi networks, a broadband router or broadband modem stores the SSID but allows administrators to change it. Routers can broadcast this name to help wireless clients find the network. Router manufacturers set a default SSID for the Wi-Fi unit, such as *Linksys, xfinitywifi, NETGEAR, dlink* or just *default.* However, since the SSID can be changed, not all wireless networks have a standard name like that.

2.4.7.2 Wireless fundamentals: Encryption and authentication

Wireless encryption and authentication help users to make an educated decision on what type of security to implement into their wireless network. There exist different types of encryption and authentication. For example, CISCO Meraki is using the following:

types of encryption and authentication	Explanations
WEP	Wired Equivalent Privacy, now depreciated, was part of the original 802.11 standard. WEP utilized a 40-128 bit key that was a combination of a key (string of hexadecimal characters) and an initialization vector. Cisco Meraki Access Points support pre-shared key WEP authentication. WEP was deemed insecure due to how easy it could be decoded but is still available in Cisco Meraki equipment for legacy devices.

WPA	Wi-Fi Protected Access, WPA, was created to "patch" the issues with WEP, allowing users to update their equipment with a firmware update as opposed to buying brand new hardware. WPA included a new type of key system called TKIP (Temporal Key Integrity Protocol.) TKIP develops a unique encryption key for each wireless frame facilitating a more secure connection. However, TKIP is susceptible to wireless attacks and is no longer considered the Enterprise standard.
WPA2 - PSK (Pre Shared Key)	WPA2 is currently the most secure standard utilizing AES (Advanced Encryption Standard) and a pre-shared key for authentication. WPA2 is backwards compatible with TKIP to allow interoperability with legacy devices. AES uses CCMP encryption protocol which is a stronger algorithm for message integrity and confidentiality. By default, SSIDs on Cisco Meraki access points that are configured as WPA2 utilize a combination of both TKIP and AES encryption.
WPA2 - Enterprise	WPA2 Enterprise utilizes authentication on a user level, using the 802.1x standard, along with the features of WPA2 such as AES. Cisco Meraki fully supports WPA2 Enterprise association with RADIUS and PEAP/MSCHAPv2, or Meraki Authentication, to provide a secure wireless network for enterprise use. Users log in with a valid username and password to authenticate instead of a pre-shared key susceptible to social engineering.
Splash Page	Cisco Meraki provides a variety of splash pages that can be utilized for additional security.

	Sign on with Authentication - Forces users to authenticate through a sign on page using various types of Authentication including RADIUS, LDAP, and Meraki Authentication. Sign on with SMS Authentication - Forces users to authenticate with an SMS code that they would receive on their phone. Systems Manager Sentry - Utilizes Cisco Meraki Systems Manager, users will need to install the manager client on their computer, their device can then be viewed on a Systems Manager network. Splash Pages can be used with or without a WPA/WEP solution as well.
Hidden SSID	A hidden SSID can prevent public visibility of your corporate SSID. Hidden SSID requires a manual creation of a wireless profile in order for the wireless client to initiate association. Although packet sniffers can detect SSID names from other probe requests and association frames, disabling SSID broadcasts can dissuade many would-be attackers from trying to gain access.

Application activity 2.4:

A. Look around your school computer lab and do the following:

- Uninstall and reinstall wireless adaptors into your desktops
- Switch on your computers and check whether wireless drivers are installed.
- Using your computers, check for available wireless signal?
- Login into your wireless router and change its SSID to “NetworkingLab”.
- What is the IP address of your computer?
- Discuss the advantages of protecting your wireless network with a password?

B. Using one smart phone, setup a computer network made of your laptops. Describe how to connect to that network. What is the name of the network? Change that name and set up a new password.

A Multistation Access Unit (MSAU) is a hub or concentrator that connects a group of computers ("nodes" in network terminology) to a token ring local area network. For example, eight computers might be connected to an MSAU in one office and that MSAU would be connected to an MSAU in another office that served eight other computers. In turn, that MSAU could be connected to another MSAU in another office, which would be connected back to the first MSAU. Such a physical configuration is called a star topology. However, the logical configuration is a ring topology because every message passes through every computer one at a time, each passing it on to the next in a continuing circle.

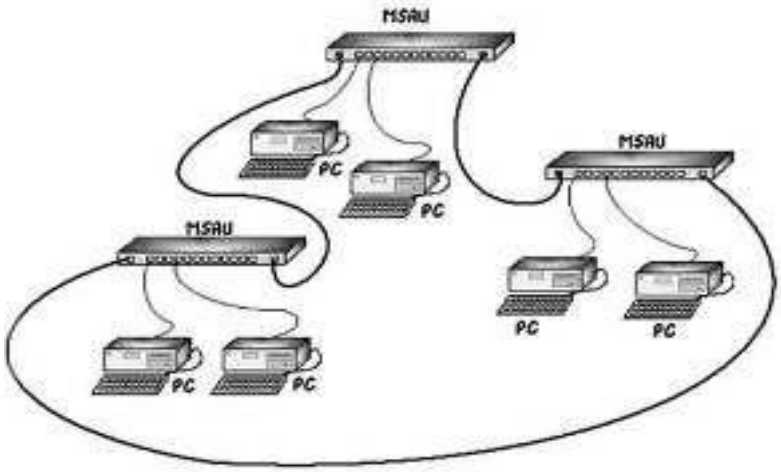


Figure 2. 3: Multistation access unit (MSAU)

Network devices

Desktop Laptop UTP cable Printer

8.NODE

A **Node** is any device on a network (server, workstation, printer, scanner, or any other kind of peripheral) that is accessed directly by the network. A node has a unique name or IP address so the rest of the network can identify it.

9. A **Client** is any machine that request something from a server. The server supplies files and sometimes processing power to the smaller machines connected to it.

10. A **Server** is any machine that can provide files, resources, or services to another machine.

11. A **Local Resource** is any peripheral (optical drive, printer, scanner, modem, and so on) that is attached to your machine. Since the machine doesn't have to go on the network to get to the device, it is called *a local device* or *a local resource*.

12. A **Network Operating System** (NOS) controls the interaction between all the machines on the network. The network operating system is responsible for controlling the way information is sent over the network medium and handles the way data from one machine is packaged and send to another. The NOS also has to handle what happens when two or more machines try to send at the same time.

13. **Concentrator**(Sometimes called "HUB"

A **Concentrator** is a device that concentrates several network connections at a single point. It is a electronic unit that converts signals coming from different slower devices to a signal that can be transmitted over faster communication-channels with a bigger bandwidth.

14. **Gateway**

A **Gateway** is a node that allows you to gain entrance into a network and vice versa. On the Internet the node which is the stopping point can be a gateway or a host node. A computer that controls the traffic your network or your ISP (Internet Service Provider) receives is a node. In most homes a gateway is the device provided by the Internet Service Provider that connects users to the internet.

15. **Backbone**

A **Backbone** is a set of nodes and links connected together comprising a network, or the upper layer protocols used in a network. A star network has no backbone.

16. **Firewall**

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software

program running on a secure host computer. A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.

17.Antenna

An antenna is an apparatus to receive or transmit radio waves and convert respectively to or from an electrical signal.

LEARNING UNIT 2 10HOURS

Apply network protocols

Learning Outcomes:

1. Describe Network Protocols

2. Describe Network standards

3. Identify and apply Network media and connectors

Learning Outcome

2.1: Describe Network Protocols

Content

• Introduction to network protocols •

Types of most common network protocols

NetBEUI

TCP/IP

Apple talk

Novell Netware(IPX/SPX)

• Description of IP terminologies

1. Describe Network Protocols

1.0 Introduction to Protocol

Just as two people can communicate successfully through the use of a single language, two computing devices can network effectively if communication is governed by the same protocol. Specifically, communication between people is accomplished through a number of norms, including accepted rules or expectations about when to listen, when to speak, appearance and acknowledgement. Likewise, computing devices need a set of rules that, when followed, result in successful network communication and data sharing: This is the purpose for protocols.

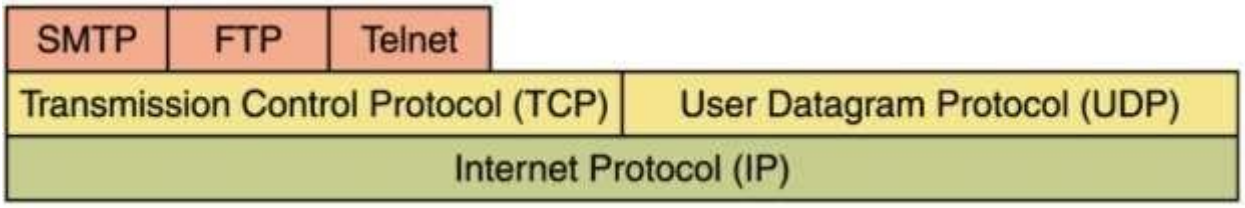
1.1. What is a Network Protocol?

A protocol is a set of rules that governs the communications between computers on a network. These rules include guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling, and speed of data transfer. In other words Communications protocols are the sets of rules by which communication over a network is achieved.

- Communications protocols are responsible for enabling and controlling network communication.
- It represents an agreement between the communicating devices. Without a protocol, 2 devices may be connected but not communicating; just like people who want to communicate but speaking different languages.
- This enables computers and software built by different people to be able to communicate in the same language.

a) Functions of network protocols are:
   - Network protocols enable computers to exchange data with each other in a meaningful, organized and efficient way.
   - They provide the path to increase the network connections
   - They enhance the data transmission rate and provide easy working to users
   - They enhance the speed of the connection

- Examples of protocols:
  - Hyper Text Transfer Protocol (HTTP) – Web Browser
  - File Transfer Protocol (FTP) – File transfer
  - Simple Mail Transfer Protocol (SMTP) – Email
  - Internet Protocol (IP) – Packets across the Internet.
- A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received.
- Network protocols are grouped such that each one relies on the protocols that underlie it sometimes referred to as a protocol stack. The key network protocols are the following:
-



- *Figure 2.52: Layering of key network protocols*

1. **A network protocol** represents a language used on the network for communication between computers. Each computer or network peripheral must use the same protocol in order to understand each other, it directs the communication process.

2. **A protocol** is a set of rules which allow defining the communication mode between two entities, software or material.

3. **A Network protocol** is a set of rules that lead communication between two computers.

Communication is the process or means by which information is sent from one place to the other.

I.2 Protocol classes

Protocols are divided into the following families:

- OSI model
- SNA (Systems Network Architecture) of IBM Company.
- DECnet architecture of DIGITAL EQUIPMENT COMPUTER Company for the establishment of DNA (Digital Network Architecture) for the local networks ETHERNET or extended networks MAN. The recent version is DECnet phase V.
- NetWare architecture for NOVELL society
- AppleTalk architecture APPLE COMPUTER Company.
- Internet model TCP/IP
- **I.3 Protocol role**
- In general protocols roles allow insuring that data is sent and received in proper format to the destination. There is no unique protocol but a set of protocols which serve communication purpose. Here are some roles of protocols:

1. **http (HyperText Transfer Protocol)**

HTTP plays a role of defining how messages are **formatted** and **transmitted**, and what actions Web servers and browsers should take in response to various commands.

2. FTP (File Transfer Protocol)

FTP protocol plays a role of **defining** the way in which data must be transferred over a TCP/IP network.
The aim of FTP protocol is to:

- allow file sharing between remote machines
- allow independence between client and server machine system files
- enable efficient data transfer

a) Four objectives of FTP are:
   - To promote sharing of files

- To encourage indirect or implicit use of computers
- To shield a user from variations in file storage systems among hosts
- To transfer data reliably and efficiently

3.IRC (Internet Relay Chat)

IRC is a real-time Internet text messaging (chat) or synchronous conferencing. It is mainly plays role in group communication in discussion forums called channels, but also it allows one to one communication via a private message as well as chat and data transfer (including file sharing.

4.Message Protocol SMTP (Simple Mail Transfer Protocol), POP (Post office Protocol) and IMAP (Internet Message Access Protocol)

SMTP: plays role of sending and receiving e-mail but it is limited to the ability of queuing messages at the receiving end.

POP : plays role of retrieving an e-mail from an e-mail server.

IMAP: Helps to access an e-mail from the local server.

IMAP stands for Internet Message Access Protocol. It is a standard protocol for accessing emails from your local server. In this protocol, emails are received and held for you by your internet server (They don't get downloaded unless when you want to read them).

POP3stands for Post Office Protocol version 3. It provides a simple, standardized way for users to access mailboxes and download messages to their computers.

5. **DNS** Domain Name Service: translates computer names into addresses and addresses into names

TCP/IP suite of protocols -TCP/IP Protocol Suite
The TCP/IP protocol suite is made of many other protocols that perform different functions. Below is a list of some of them:

TCP/IP stands for *Transmission Control Protocol/Internet Protocol*. It is a set of network protocols, which enable the computers over a network to communicate with each other. TCP/IP is a protocol suite, which is named after the pair of its two most important protocols, **TCP** and **IP**:

- **IP**: On a TCP/IP network, before a message is sent, it is broken into chunks of information called Packets. Each packet is given the IP Address of the sender and destination machine. Based on those IP Addresses, the IP part of TCP/IP is responsible for determining the path each packet of data has to take to reach its destination. Each packet may take its own path because all packets will be unified at the destination machine to make the original message. IP is responsible for "routing" each packet to the correct destination.

  IP - This is a connectionless protocol, which means that a session is not created before sending data. IP is responsible for addressing and routing of packets between computers. It does not

guarantee delivery and does not give acknowledgement of packets that are lost or sent out of order as this is the responsibility of higher layer protocols such as TCP.

- **TCP** - is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

  TCP - TCP breaks data into manageable packets and tracks information such as source and destination of packets. It is able to reroute packets and is responsible for guaranteed delivery of the data.

Other protocols include:

- **File Transfer Protocol (FTP)**

The FTP is used on networks based on TCP/IP model to upload and download individual files to or from a file server to your client machine.
FTP - File transfer protocol is used for transferring files between remote systems. Must resolve host name to IP address to establish communication. It is connection oriented (i.e. verifies that packets reach destination).

- **Trivial File Transfer Protocol (TFTP)**

It is same as the FTP but with limited functions in it . The main advantage is that it can be implemented using small memory. It found its application in the old days as computer internal memory was limited. Just like FTP it is used to transfer files. Because of being smaller in size it has its own disadvantages also like it cannot download files up to a size of 1 Terabyte and has no security mechanism.
TFTP - Same as FTP but not connection oriented.

- **Simple Mail Transfer Protocol (SMTP) or Extended SMTP (ESMTP)**

This protocol is used for sending e-mail from your client machine to the mail server. Email is the electronic message sent from one computer to another on a network/internet.

- **Post Office Protocol (POP)**

The POP protocol is used by email programs (like Microsoft Outlook) to retrieve emails from an email server. If your email program uses POP, all your emails are downloaded to your email program (also called email client), each time it connects to your email server.POP stands for Post Office protocol. This protocol as the name suggests is used for the purposes of mailing.

POP3 is a new version of Post office protocol which is also being used as POP.
Post Office Protocol. A POP3 mail server holds mail until the workstation is ready to receive it

IMAP (Internet Message Access Protocol)

The IMAP protocol is used by email programs (like Microsoft Outlook) just like the POP protocol.

The main difference between the IMAP protocol and the POP protocol is that the IMAP protocol will not automatically download all your emails each time your email program connects to your email server.

The IMAP protocol allows you to look through your email messages at the email server before you download them. With IMAP you can choose to download your messages or just delete them. This way IMAP is perfect if you need to connect to your email server from different locations, but only want to download your messages when you are back in your office.

IMAP - Like POP3, Internet Message Access Protocol is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server.

- **HTTP (Hypertext Transfer Protocol)**

To understand what http is, it is very important to first understand the following terms:

- ✓ *HTML (Hypertext Markup Language)*

This is a programming language used to format (or simply to create) electronic documents viewable on internet. This language uses codes called **tags** with **attributes**. Each HTML page may consist of hypertext, graphics, audio and/or video.

- ✓ *Hypertext*

It is a text with **built-in hyperlinks** or **links** to other web pages.

- ✓ *Hyperlink*

A hyperlink or a link simply means a reference to another web page within the same website or a link to another website. This means that you can jump from one document to another by simply clicking on a link.

- ✓ *Web page*

Each electronic document formatted in HTML is called a webpage

- ✓ *Website*

A web site is a collection of related web pages

- ✓ *Homepage*

The first web page of the website is called a **homepage** or **index** page. It normally contains important links that link to other web pages of the same website, or to other websites. We can think of a home page as a table of contents of a book.

- ✓ *Web server*

A server that hosts one or more websites is called a web server.

- ✓ *www*

This stands for **World Wide Web** or simply the **Web.** WWW is a system of web servers interconnected among them and of course connected to internet. The WWW has become the biggest collective pool of knowledge today.

Note: Not all Internet servers are part of the World Wide Web because all of them are not web servers, that is why *World Wide Web* is **not** synonymous with *the Internet*. Also a web does not mean a **website.**

Now, what is http?

http is a protocol used by a web browser to fetch a webpage from a web server, i.e. this protocol is uniquely used to retrieve an html page from a web server to be displayed by the client machine.

HTTP - The Hypertext Transfer Protocol is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. It is the protocol controlling the transfer and addressing of HTTP requests and responses.

HTTPS - Signifies that a web page is using the Secure Sockets Layer (SSL) protocol and is providing a secure connection. This is used for secure internet business transactions

Telnet

Telnet stands for Teletype Network . Telnet can be used on the operating systems command line interface .This protocol can be used on the internet . It was developed in the late 1960s . Telnet versions are available for all operating systems . It is a client server based protocol and is a connection oriented protocol . Telnet lags behind in the security issues as telnet doesn't support encryption of data while transmission . It also doesn't have support for authentication TELNET - Provides a virtual terminal or remote login across the network that is connection-based. The remote server must be running a Telnet service for clients to connect

SNMP

SNMP stands for Simple Network Management Protocol (SNMP) . It is network protocol . This protocol as the name suggests is used in networks for the management of network devices . The devices connected on the network can be administered through the simple network management protocol by the network administrator .

NTP - Network Time Protocol is a protocol that is used to synchronize computer clock times in a network of computers.

UDP: stands for User Datagram Protocol . Using UDP as the name suggests , the computers can send messages on the internet . The messages in UDP are called datagram . The UDP works on a network supporting the IP internet protocol. It doesn't support reliable service . The service supported by UDP is unreliable type. Error checking and correction is not supported in UDP. UDP is typically used in applications which are time sensitive. Here the user can afford to have error but not delay in the reaching of packets. For error checking some other protocol has to be used . UDP supports multicasting and broadcasting or data packets on the network. • For example video and voice are the kind or data which can afford to have some error or loss in packet sequence but not delay in reception . Quality may go down for a small interval due to the above mentioned problems but the continuity of the video is not broken which is important

UDP - A connectionless, datagram service that provides an unreliable, best-effort delivery.

ARP - provides IP-address to MAC address resolution for IP packets. A MAC address is your computer's unique hardware number and appears in the form 00-A0-F1-27-64-E1 (for example). Each computer stores an ARP cache of other computers ARP-IP combinations.

- *Address Resolution Protocol (ARP) finds the hardware address of a host from a known IP* address.

ICMP - Internet Control Message Protocol enables systems on a TCP/IP network to share status and error information such as with the use of PING and TRACERT utilities.

DHCP : stands for Dynamic Host Configuration Protocol and provides a solution that automatically assigns IP addresses to computers on a network. When a client is configured to receive an IP address automatically, It will send out a broadcast to the DHCP server requesting an address. The server will then issue a "lease" and assign it to that client. The time period that a lease will last can be specified on the server

Some of the benefits of DHCP include the following:

Prevents users from making up their own IP addresses.

Prevents incorrect gateway or subnet masks from being entered by your helpdesk.

Decreases amount of time spent configuring computers especially in environments where computers get moved around all the time.

Handy in situations where you have a large sales staff that only have to work 1 day a week. On that one day they bring their laptops and they can just plug them into the network and they are all set.

NAT/ICS

NAT stands for Network Address Translation/ Internet Connection Sharing and is a commonly used IP translation and mapping technology. Using a device (such as a router) or piece of software that implements NAT allows an entire home or office network to share a single internet connection over a single IP address. A single cable modem, DSL modem, or even 56k modem could connect all the computers to the internet simultaneously.

Some of the protocols used on the internet are :- 1. TCP 2. IP 3. DNS 4. FTP 5. TFTP 6. UDP 7. SNMP 8. POP3 9. IMAP 10. HTTP 11. NFS 12. MIME 13. SSL 14. ICMP 15. IGMP

2 Most used protocols

The most used protocols with their descriptions are given in the following table.

Protocol Name	Description
a) Simple Mail Transfer Protocol (SMTP)	The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. Client software uses Internet Message Access Protocol (IMAP) or Post Office Protocol (POP) protocols to receive emails.
b) File Transfer Protocol (FTP)	The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. It is the standard mechanism provided by TCP/IP for copying a file from one host to another.
c) TErminaL NETwork (TELNET)	TELNET is an abbreviation for TErminaL NETwork. It is the standard TCP/IP protocol for virtual terminal service as proposed by the International Organization for Standards (ISO). TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

d) Transmission Control Protocol /Internet Protocol (TCP/IP)	TCP stands for "Transmission Control Protocol" TCP software breaks messages into packets, hands them off to the IP software for delivery, and then orders and reassembles the packets at their destination IP stands for Internet Protocol Internet Protocol (IP) is the principal set of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks, using the Internet Protocol Suite (often referred to as TCP/IP). TCP/IP The Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the Internet. It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the Internet. TCP/IP can also be used as a communication protocol in a private network (an intranet or an extranet).
e) User Datagram Protocol (UDP)	It is an alternative to TCP. The main difference is that TCP is highly reliable, at the cost of decreased performance, while UDP is less reliable, but generally faster.

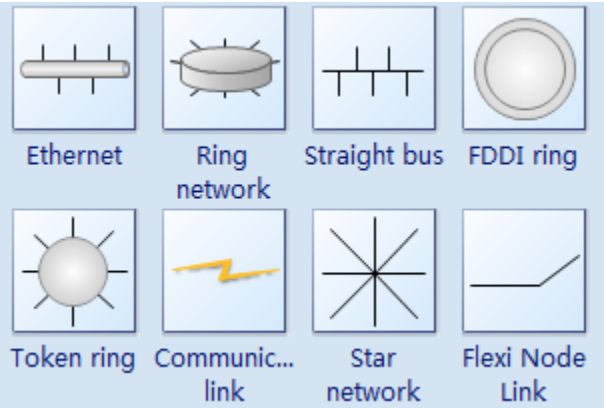
f) Post Office Protocol version 3 (POP3)	Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client. POP3 allows you to download email messages on your local computer and read them even when you are offline. Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server. By default, the POP3 protocol works on two ports: Port 110 - this is the default POP3 non-encrypted port Port 995 - this is the port you need to use if you want to connect using POP3 securely
g) Internet Message Protocol (IMAP)	The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers. While the POP3 protocol assumes that an email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable for the user if he/she is going to access his/her email from different locations or if his/her messages are managed by multiple users. By default, the IMAP protocol works on two ports: Port 143 - this is the default IMAP non-encrypted port Port 993 - this is the port someone needs to use if he/she wants to connect using IMAP securely.

h) Dynamic Host Configuration Protocol (DHCP)	Dynamic Host Configuration Protocol (DHCP) is a protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
i) Hypertext Transfer Protocol (HTTP)	The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions as a combination of FTP and SMTP.
j) Hypertext Transfer Protocol Secure (HTTPS)	Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. It means that all communications between your browser and the website are encoded. HTTPS is often used to protect highly confidential online communications like online banking and online shopping order forms. Web browsers such as Internet Explorer, Firefox and Chrome also display a padlock icon in the address bar to visually indicate that a HTTPS connection is in effect.
k) Secure Shell (SSH)	The Secure Shell (SSH) protocol is a method for securing remote login from one computer to another. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).
l) Some of the other most used protocols	Network Basic Input/output System (NetBIOS) NetBIOS Extended User Interface (NetBEUI) Address Resolution Protocol (ARP) Domain Name System (DNS) Internet Control Message Protocol (ICMP) Internet Group Management Protocol (IGMP) Internet Message Access Protocol version 4 (IMAP4) Trivial File Transfer Protocol (TFTP)

1.2. Types of Network Protocols

The most common network protocols are:

- ✓ Ethernet
- ✓ Local Talk
- ✓ Token Ring
- ✓ FDDI
- ✓ ATM
- ✓ The follow is some common-used network symbols to draw different kinds of network protocols.



Ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

The Ethernet protocol allows for linear bus, star, or tree topologies. Data can be transmitted over wireless access points, twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps up to 1000 Mbps.

Fast Ethernet

To allow for an increased speed of transmission, the Ethernet protocol has developed a new standard that supports 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary. Fast Ethernet is becoming common in schools that have been recently wired.

Local Talk

Local Talk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by Local Talk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. Local Talk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

The Local Talk protocol allows for linear bus, star, or tree topologies using twisted pair cable. A primary disadvantage of Local Talk is speed. Its speed of transmission is only 230 Kbps.

Token Ring

The Token Ring protocol was developed by IBM in the mid-1980s. The access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the increasing popularity of Ethernet, the use of Token Ring in school environments has decreased.

FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

ATM

Asynchronous Transfer Mode (ATM) is a network protocol that transmits data at a speed of 155 Mbps and higher. ATM works by transmitting all data in small packets of a fixed size; whereas, other protocols transfer variable length packets. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology, which can work with fiber optic as well as twisted pair cable. ATM is most often used to interconnect two or more local area networks. It is also frequently used by Internet Service Providers to utilize high-speed access to the Internet for their clients. As ATM technology becomes more cost-effective, it will provide another solution for constructing faster local area networks.

Gigabit Ethernet

The most recent development in the Ethernet standard is a protocol that has a transmission speed of 1 Gbps. Gigabit Ethernet is primarily used for backbones on a network at this time. In the future, it will probably be used for workstation and server connections also. It can be used with both fiber optic cabling and copper. The 1000BaseTX, the copper cable used for Gigabit Ethernet, is expected to become the formal standard in 1999.

Compare the Network Protocols

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star
Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

Internet protocol (IP) and Transmission Control Protocol (TCP)

IP (Internet Protocol) is the primary network protocol used on the Internet, developed in the 1970s. On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP.

IP supports unique addressing for computers on a network. Most networks use the Internet Protocol version 4 (*IPv4*) standard that features IP addresses four bytes (32 bits) in length. The newer Internet Protocol version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length.

Data on an Internet Protocol network is organized into *packets*. Each IP packet includes both a header (that specifies source, destination, and other information about the data) and the message data itself.

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets: A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.) that a message is divided into for efficient routing through the Internet.

TCP is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Types of most common network protocols

NetBEUI

TCP/IP

Apple talk

Novell Netware(IPX/SPX)

TCP/IP - TCP/IP is the protocol suite of the internet and will be covered in the next section. IPX/SPX - These protocols were developed by Novell and are/were used with Novell Netware. IPX is the fastest routable protocol and is not connection oriented. IPX addresses are up to 8 characters in hexadecimal format. SPX is connection oriented.

NetBeui - Stands for "NetBIOS Extended User Interface". It is a transport layer protocol mainly used for small Windows 9x and NT LANs. In reference to the NetBIOS distinction, NetBIOS is the applications programming interface and NetBEUI is the transport protocol. NetBEUI is a non-routable protocol meaning it will not allow communication through a router. It is broadcast oriented which causes it to not scale well. Although it can still be installed on newer Microsoft operating systems, it has largely been replaced by TCP/IP.

Appletalk - AppleTalk is the name given to the set of protocol and networking standards created by Apple Computer for use with the Macintosh family of computers.

AppleTalk is routable and automatically handles such things as assigning of workstation and network addresses, message routing between networks, etc.

1. **NetBEUI**

- NetBEUI is the protocol that is responsible for data transport. Does handle all the frame formatting that is not handled by NetBIOS.

is an enhanced version of the NetBios**protocol** that is used by Microsoft Windows networking. It is a non-routable **protocol**, which means that computers that are not located on the same network segment or subnet can't communicate.

What is NetBEUI?

NetBEUI stands for NetBIOS Extended User Interface, is a networking protocol developed by IBM and Microsoft in 1985 that is used for workgroup-size local area networks (LANs) with up to 200 stations. NetBEUI is an extension of the NetBIOS protocol.

NetBEUI was the primary protocol for LAN Manager and Windows for Workgroups. It is a fast and efficient protocol with low overhead that supports both connection-oriented communication (such as communication for mapping drives using the Net Use command and starting services remotely using the Net Start command) and connectionless communication (such as communication for sending datagrams, registering NetBIOS names, and performing NetBIOS name resolution).

NetBEUI is also self-tuning and implements flow control and error detection. It defines a framing mechanism at the transport layer and implements the LLC2 protocol of the Open Systems Interconnection (OSI) reference model for networking.

2.TCP/IP

TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

The two main protocols in the internet protocol suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

How TCP/IP works

TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

3.APPLETALK

AppleTalk is a discontinued proprietary suite of networking protocols developed by Apple Inc. for their Macintosh computers. AppleTalk includes a number of features that allow local area networks to be connected with no prior setup or the need for a centralized router or server of any sort. Connected AppleTalk-equipped systems automatically assign addresses, update the distributed namespace, and configure any required inter-networking routing.

AppleTalk was released in 1985, and was the primary protocol used by Apple devices through the 1980s and 1990s. Versions were also released for the IBM PC and compatibles and the Apple IIGS. AppleTalk support was also available in most networked printers (especially laser printers), some file servers, and a number of routers.

The rise of TCP/IP during the 1990s led to a reimplementation of most of these types of support on that protocol, and AppleTalk became unsupported as of the release of Mac OS X v10.6 in 2009. Many of AppleTalk's more advanced autoconfiguration features have since been introduced in Bonjour, while Universal Plug and Play serves similar needs

4.NOVELL NETWARE(IPX/SPX)

NetWare is a **network** operating system developed by **Novell**, which allows the**networking** of **computers**, be it DOS, Windows, Unix or Mac OS. ... In 1983, when he

designed the first version of **NetWare**, all other competing products were based on the concept of providing direct access to shared disks.

IPX (Internetwork Packet Exchange) is a networking **protocol** from Novell that interconnects networks that use Novell's NetWare clients and servers. **IPX** is a datagram or packet **protocol**.

IPX (Internetwork Packet Exchange) is a networking protocol from Novell that interconnects networks that use Novell's NetWare clients and servers. IPX is a datagram or packet protocol. IPX works at the Network layer of communication protocols and is connectionless (that is, it doesn't require that a connection be maintained during an exchange of packets as, for example, a regular voice phone call does).

Internetwork Packet Exchange/Sequenced Packet Exchange (**IPX**/**SPX**) is a set of network **protocols** that provide packet switching and sequencing for small and large networks. **IPX** works at layer three of the Open Systems Interconnection (OSI) model and **SPX** works at layer 4.

IPX/SPX stands for Internetwork Packet Exchange/Sequenced Packet Exchange. IPX and SPX are networking protocols used initially on networks using the Novell NetWare operating systems, but became widely used on networks deploying Microsoft Windows LANS, as they replaced NetWare LANS.

IPX and SPX are derived from Xerox Network Systems' IDP and SPP protocols, respectively. IPX is a network layer protocol (layer 3 of the OSI Model), while SPX is a transport layer protocol (layer 4 of the OSI Model). The SPX layer sits on top of the IPX layer and provides connection-oriented services between two nodes on the network. SPX is used primarily by client–server applications.

IPX and SPX both provide connection services similar to TCP/IP, with the IPX protocol having similarities to IP, and SPX having similarities to TCP. IPX/SPX was primarily designed for local area networks (LANs), and is a very efficient protocol for this purpose (typically SPX's performance exceeds that of TCP on a small LAN,[citation needed] as in place of congestion windows and confirmatory acknowledgements, SPX uses simple NAKs). TCP/IP has, however, become the de facto standard protocol. This is in part due to its superior performance over wide area networks and the Internet (which uses TCP/IP exclusively), and also because TCP/IP is a more mature protocol[citation needed], designed specifically with this purpose in mind.

Internetwork (Internet, Intranet, Extranet)

ACTIVITY 3.5

Using computer network, an organization’s employees can access data when they are inside the organization buildingand when they are physically outside. Investigate technologies that can be used to allow employees inside and outside to access organization’s data.

A network of networks is called an internetwork, or simply the **Internet**. The Internet, extranets, and intranets all rely on Transport Control Protocol / Internet Protocol (TCP/IP).

However, they are different in terms of the levels of access they allow to various users inside and outside the organization and the size of the network.

1. **An Intranet** is a private computer network that uses Internet Protocol to securely share any part of an organization's information or operational systems within that organization. Only users inside the organization are only allowed to access it.
2. **An Extranet** is a private network that uses Internet protocols, network connectivity. An extranet can be viewed as part of a company's intranet that is extended to users outside the company, the connectivity is made possible by the Internet.
3. **The Internet** is a global system of interconnected computer networks that use the standard Internet Protocol suite (TCP/IP) to serve billions of users worldwide.

The difference between the Internet and Extranets is that while the extranet allows limited access to non-members of an organization, the Internet generally allows everyone to access all network resources.

4. **The OSI Seven(7)-Layer Model**/OSI model

- Before communication can occur between two computers numerous operations operate behind the scene. The computing community has set on several standards and specifications that define the interaction and interrelation of the various components of network architecture.
- In 1977 the International standards organization called ISO, initiated efforts to design a communication standard based on the open systems architecture theory from which computer networks would be designed. This model was known as the Open Systems Interconnection (OSI) model. This model has become an accepted framework for analyzing and developing networking components and functionality.
- The OSI model was first released in 1984 by the international standards organization (ISO), it provides a useful structure for defining and describing the various processes underlying networking communications.
- The OSI model organizes communication protocols into seven levels. Each level addresses a narrow portion of the communication process.

When two systems communicate on the network, information is sent down through the protocol stack of one system, over the cable and then up through the protocol stack to the appropriate layer on the other system

Layer	Functionality
7. Application	Network services, authentication
6. Presentation	Translation, encryption
5. Session	Connections, sessions
4. Transport	Fragmentation, defragmentation, reliable data delivery, error correction/management, flow control
3. Network	Addressing, routing
2. Data Link	Packets/Frame, CRC generation/checking, network access
1. Physical	Media, connectors, electrical signals

What is the purpose of the OSI model?

- The *OSI model* was established to *standardize* the design and construction of computer networks for developers and hardware manufacturers. Standards allow hardware and software components from a variety of different vendors to operate together**.**

- **IBM mainframes use *Systems Network Architecture (SNA)* that is a set of layered protocols like the OSI model. However, the SNA layers are not directly comparable to the OSI model layers. This makes interoperability between PC-based networks and IBM mainframes more difficult.**
- **Important concepts to understand OSI layering are:**
  - **Each layer performs unique and specific task.**
  - **A layer only has knowledge of its immediately adjacent layers.**
  - **A layer uses services of the layer below.**
  - **A layer performs functions and provides services to the layer above.**

- The application layer is unique among the seven layers in that, it has no layer above.
- Each layer contains functions that provide specific services for facilitating a communication.
- The OSI model is a framework that describes how a function from one computer is transmitted to another computer on the network.
- When information is passed within the OSI model on a computer, each protocol layer adds its own information to the message being sent.
- A header is added to the beginning of the original message.
- When the message is received by the destination computer, each layer removes the header from the peer layer.
- The headers are stripped in the reverse order in which they were added. The last header added by the sending computer is the first one stripped off and read by the receiving computer.
- The information between layers is passed along vertically, but the information between computers is essentially horizontally.

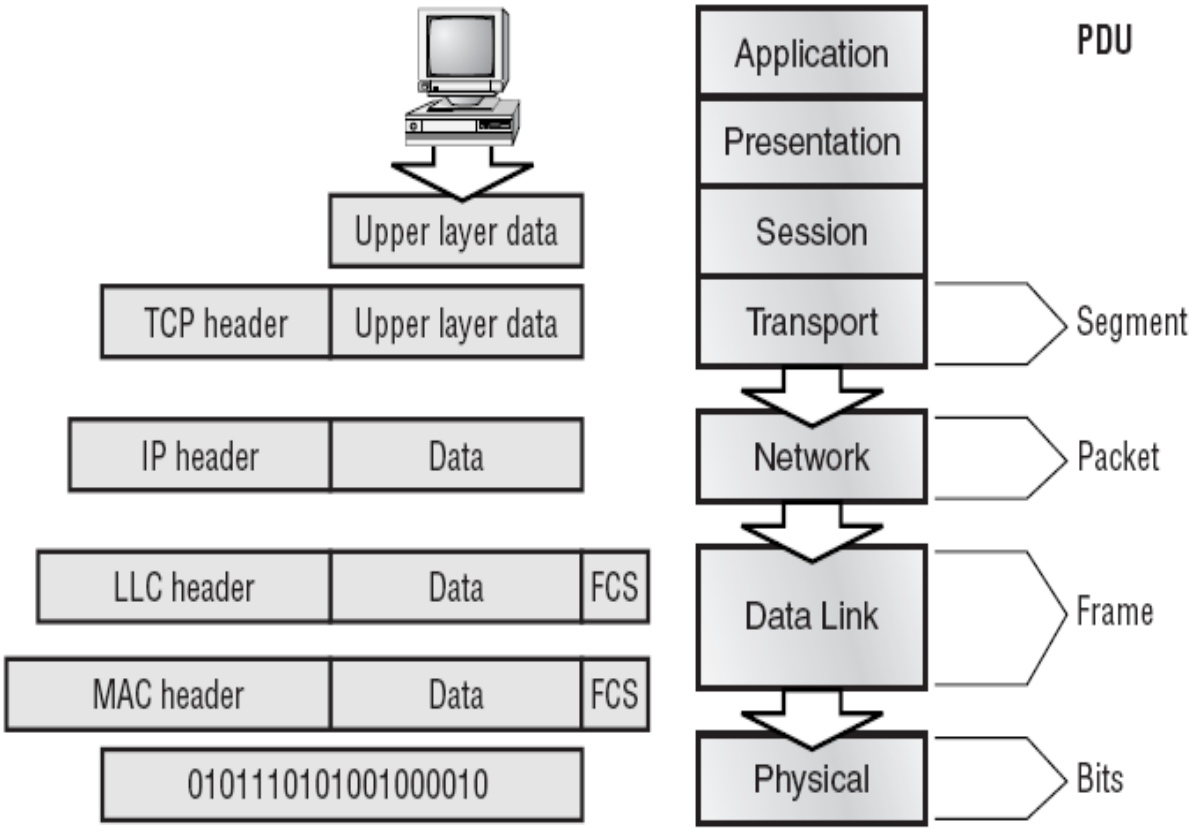
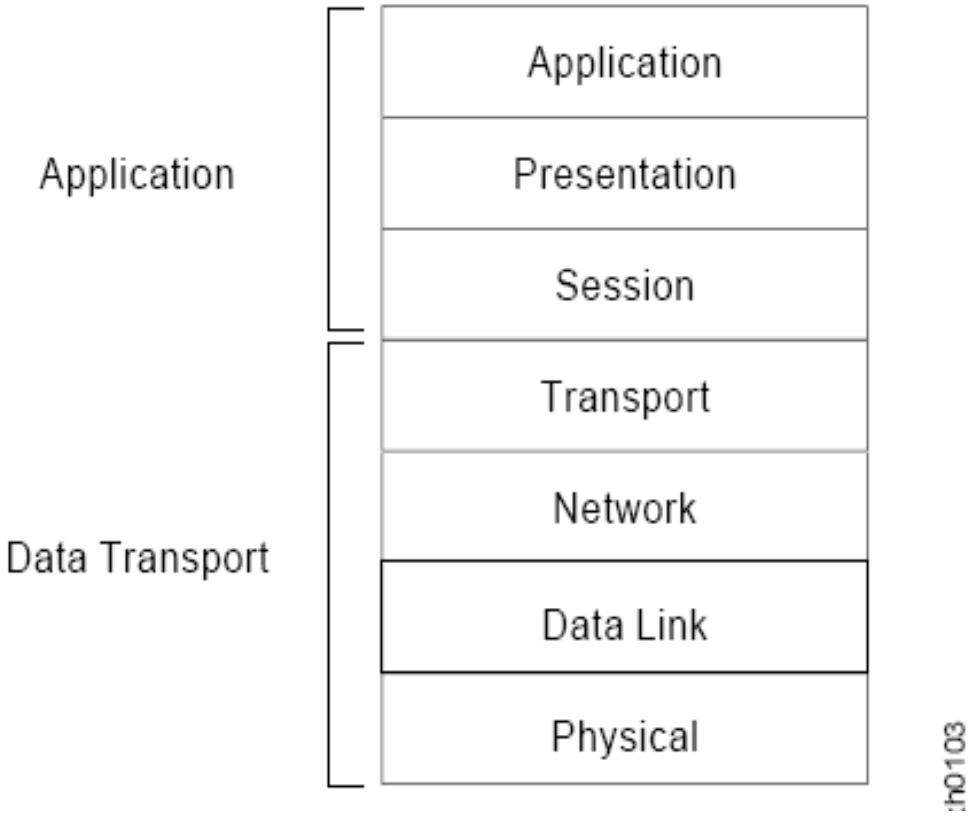


Figure 1-3 Two sets of layers make up the OSI layers.



Open System Interconnect (OSI) is an open standard for all communication systems. OSI model is established by International Standard Organization (ISO). It is a general-purpose model for discussing or describing how computers communicate with one another over a network. Its sevenlayered approach to data transmission divides the many operations up into specific related groups of actions at each layer.

Table 2. 5: Data flow in OSI layers

Transmitting de ice				Receiving device
Application software				Application software
↓	7	Application	7	↑
↓	6	Presentation	6	↑

↓	5	Session	5	↑
↓	4	Transport	4	↑
↓	3	Network	3	↑
↓	2	Data link	2	↑
↓	1	Physical	1	↑

In the OSI model, data flows down the transmit layers, over the physical link, and then up through the receive layers. The transmitting computer software gives the data to be transmitted to the applications layer, where it is processed and passed from layer to layer down the stack with each layer performing its designated functions. The data is then transmitted over the physical layer of the network until the destination computer or another device receives it. At this point the data is passed up through the layers again, each layer performing its assigned operations until the data is used by the receiving computer's software. The roles of OSI model layers are:

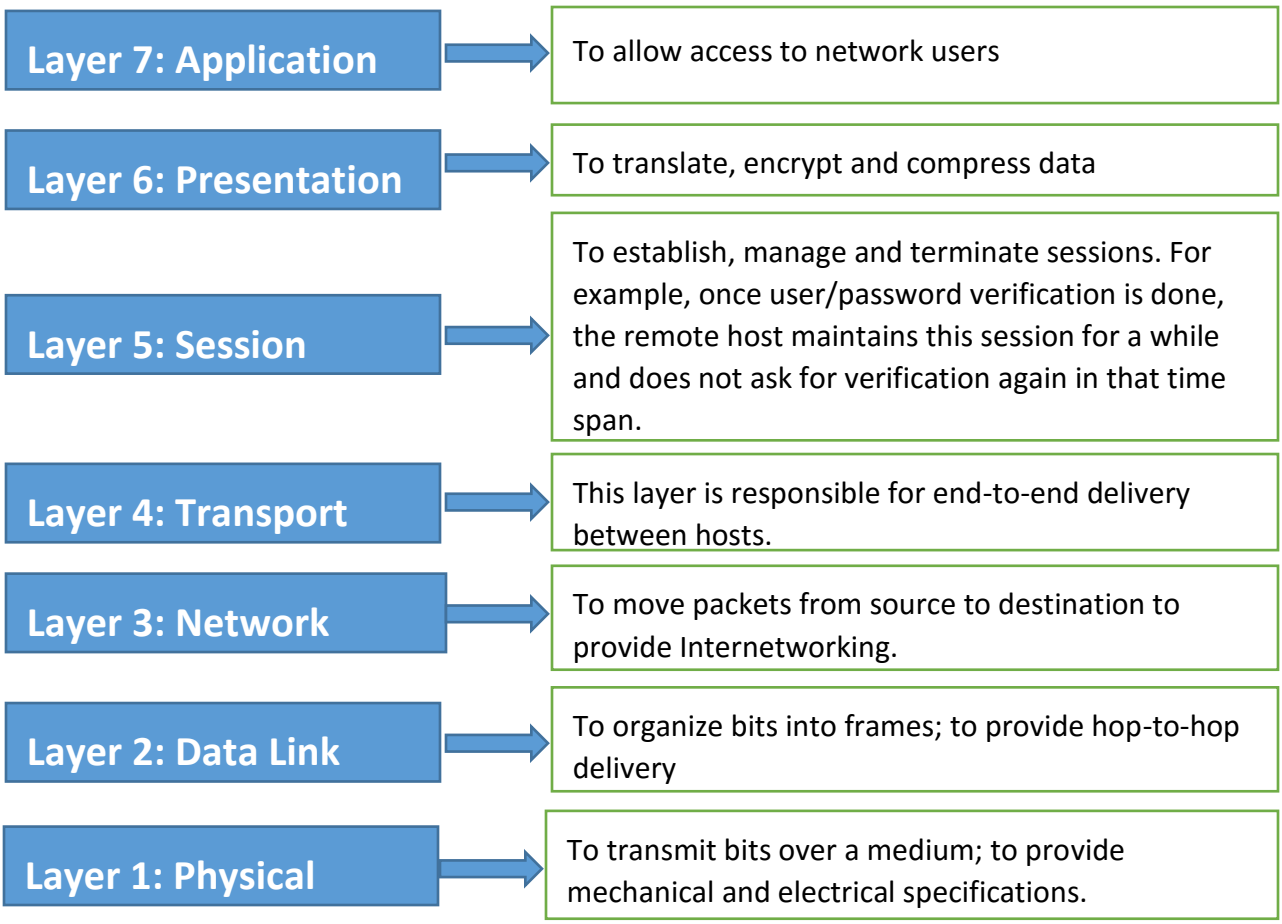


Figure 2.57: Layers in OSI Model

a) The Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as domain name service (DNS), file transfer protocol (FTP), hypertext transfer protocol (HTTP), Internet message access protocol (IMAP), post office protocol (POP), simple mail transfer protocol (SMTP), Telenet, and terminal emulation. Devices used in this layer are Gateways, Firewalls, and all end devices like PC's, Phones, and Servers.

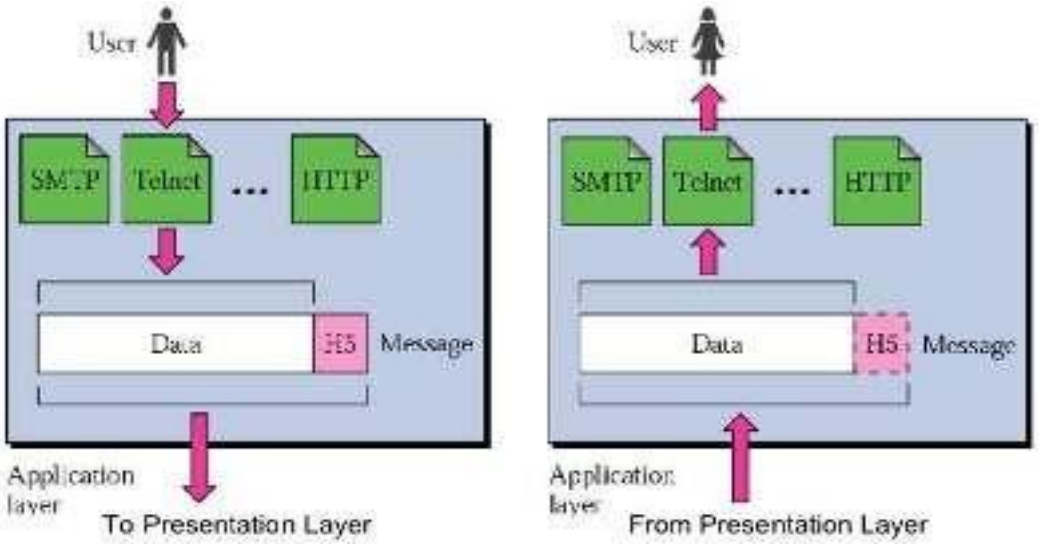


Figure 2.58: Application layer

b) The Presentation Layer

It presents data to the Application layer and is responsible for data translation and code formatting. The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

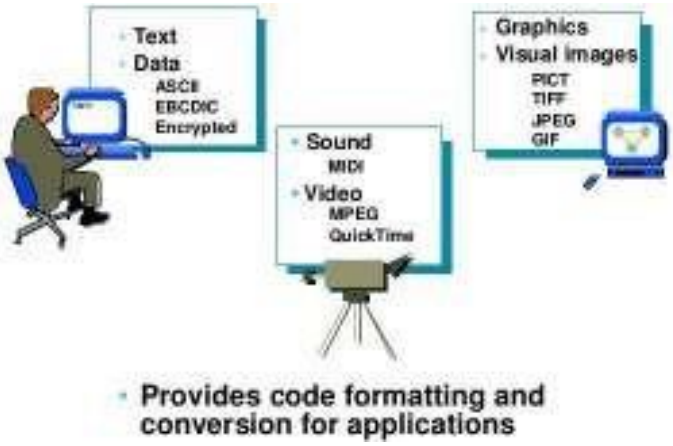


Figure 2.59: Presentation layer

Specific responsibilities of the presentation layer include the following:

- Translation
- Encryption
- Compression

Devices which operate at this layer are Gateways, Firewalls and PC's.

c) The Session Layer

The *Session layer* is responsible for setting up, managing, and then destroying down sessions between Presentation layer entities. This layer also provides dialogue control between devices, or nodes.

It coordinates communication between systems and serves to organize their communication by offering three different modes: *simplex, half duplex*, and *full duplex*.

Figure 2.60: Session layer

Specific responsibilities of the session layer include the following:

- Dialog control
- Synchronization

The devices used at this layer are Gateways, Firewalls, and PC's.

d) The Transport Layer

The *Transport layer* segments and reassembles data into a data stream. Services located in the transport layer segment and reassemble data from upper-layer applications and unite it onto the same data stream. They provide end-to-end data transport services and can establish a logical connection between the sending host and destination host on an Internetwork. At this layer we find devices like Gateways and Firewalls.

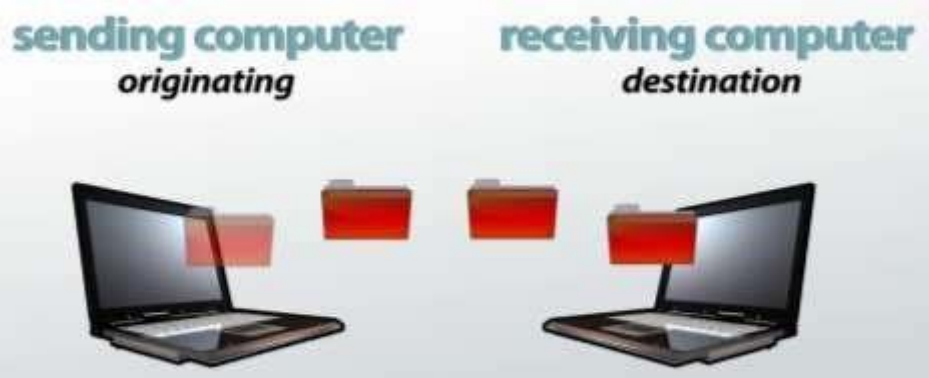


Figure 2.61: Transport layer

e) The Network Layer

The *Network layer* manages device addressing, tracks the location of devices on the network, and determines the best way to move data, which means that the Network layer must transport traffic between devices that are not locally attached. Routers (layer 3 devices) are specified at the Network layer and provide the routing services within an Internetwork.

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Two activities are performed:

- **Logical addressing**: IP addressing
- **Routing**: Source to destination transmission between networks

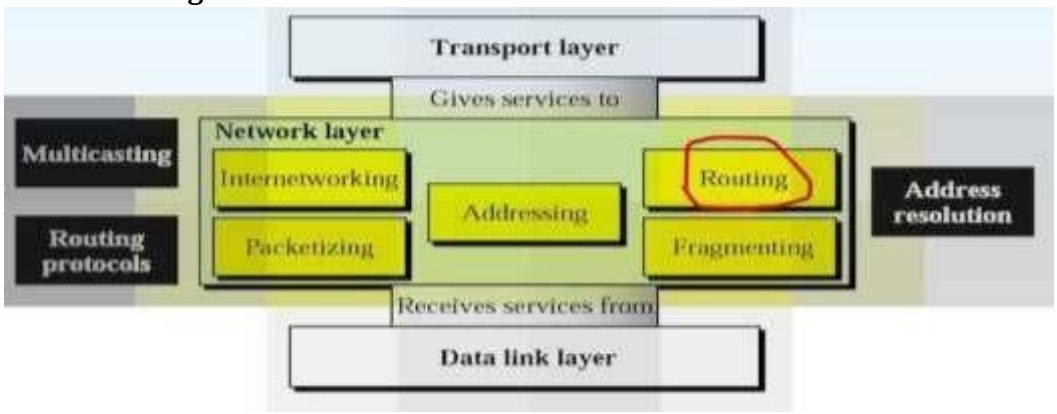


Figure 2.62: Network layer

f) The Data Link Layer

The Data Link layer formats the message into pieces, each called a ***data frame***, and adds a customized header containing the hardware destination and source address. This added information forms a sort of capsule that surrounds the original message.

To allow a host to send packets to individual hosts on a local network as well as transmit packets between routers, the Data Link layer uses hardware addressing.

Switches and bridges work at the Data Link layer and filter the network using hardware (MAC) addresses.

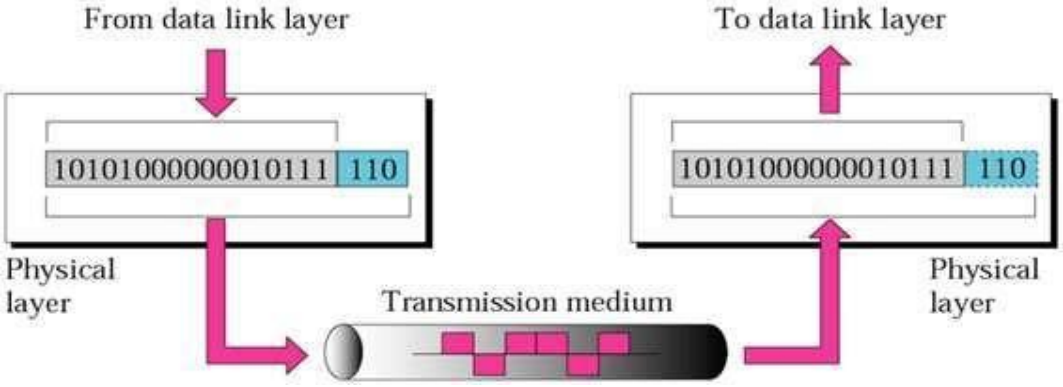


Figure 2.63: Data Link layer

f) The Physical Layer

Finally arriving at the bottom, we find that the *Physical layer* does two things: It sends bits and receives bits. Bits come only in values of 1 or 0. The Physical layer communicates directly with the various types of actual communication media.

The Physical layer specifies the electrical, mechanical, procedural, and functional requirements for activating, maintaining, and deactivating a physical link between end systems. This layer is also where you identify the interface between the data terminal equipment (DTE) and the data communication equipment (DCE).

Devices like Hubs, Repeaters, Cables, and Fibers operates at this layer.

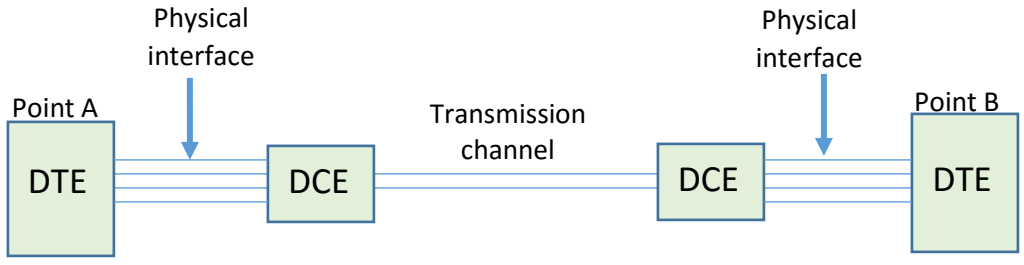


Figure 2.64: Physical layer

Notice that the following network devices operate on all seven layers of the OSI model:

- Network management stations (NMSs)

- Web and application servers
- Gateways (not default gateways)
- Network hosts

2.6.2 Advantages of using the OSI layered model

1. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
2. It allows multiple-vendor development through standardization of network components.
3. It encourages industry standardization by defining what functions occur at each layer of the model.
4. It allows various types of network hardware and software to communicate.
5. It prevents changes in one layer from affecting other layers, so it does not hamper hardware or software development.

Application activity:

1. Which layer of the OSI model creates a virtual link between hosts before transmitting data?
2. What is the main reason of the creation of OSI model?
3. Describe each one of the 7 layers of the OSI model.
4. Which layer is responsible for converting data packets from the Data Link layer into electrical signals?
5. At which layer is routing implemented, enabling connections and path selection between two end systems?

6. Which layer defines how data is formatted, presented, encoded, and converted for use on the network?
7. Which layer is responsible for creating, managing, and terminating sessions between applications?
8. Search on Internet and propose the format of a packet sent between 2 computers through the layers of the OSI model.

. Short description of OSI layers

a. Application: To allow access to network users

b. Presentation: To translate, encrypt and compress data

c. Session: To establish, manage and terminate sessions. For example, once user/password verification is done, the remote host maintains this session for a while and does not ask for verification again in that time span.

d. Transport: This layer is responsible for end-to-end delivery between hosts.

e. Network: To move packets from source to destination to provide internetworking.

f. Data link: To organize bits into frames; to provide hop-to-hop delivery

g. Physical: To transmit bits over a medium; to provide mechanical and electrical specifications

The OSI networking model is divided into 7 layers. Each layer has a different responsibility, and all the layers work together to provide network data communication.

Physical - The Physical layer is the specification for the hardware connection, the electronics, logic circuitry, and wiring that transmit the actual signal. It is only concerned with moving bits of data on and off the network medium. Most network problems occur at the Physical layer.

Data Link - The Data Link layer is the interface between the upper "software" layers and the lower "hardware" Physical layer. One of its main tasks is to create and interpret different frame types based on the network type in use. The Data Link layer is divided into two sub-layers:

the Media Access Control (MAC) sub-layer and the Logical Link Control (LLC) sub-layer.

LLC sub-layer starts maintains connections between devices (e.g. server - workstation).

MAC sub-layer enables multiple devices to share the same medium. MAC sub-layer maintains physical device (MAC) addresses for communicating locally (the MAC address of the nearest router is used to send information onto a WAN).

Network - The Network layer addresses messages and translates logical addresses and names into physical addresses. It also manages data traffic and congestion involved in packet switching and routing.

It enables the option of specifying a service address (sockets, ports) to point the data to the correct program on the destination computer.

Transport - The Transport layer provides flow control, error handling, and is involved in correction of transmission/reception problems. It also breaks up large data files into smaller packets, combines small packets into larger ones for transmission, and reassembles incoming packets into the original sequence.
Session - The Session layer handles security and name recognition to enable two applications on different computers to communicate over the network. Manages dialogs between computers by using simplex(rare), half-duplex or full-duplex. The phases involved in a session dialog are as follows: establishment, data-transfer and termination.

Presentation- The Presentation layer determines data exchange formats and translates specific files from the Application layer format into a commonly recognized data format. It provides protocol conversion, data translation, encryption, character-set conversion, and graphics-command expansion.
Application - The Application layer represents user applications, such as software for file transfers, database access, and e-mail. It handles general network access, flow control, and error recovery. Provides a consistent neutral interface for software to access the network and advertises the computers resources to the network.

Here is an idiotic, yet easy way to remember the 7 layers. Memorize the following sentence: All People Seem To Need Data Processing. The first letter of each word corresponds to the first letter of the layers starting with Application and ending with the physical layer.

Here are some examples of items that operate at each layer:

Layer	Device
Application	Gateway
Presentation	Gateway
Session	Gateway
Transport	Gateway
Network	Routers, Layer 3 Switches
Data Link	Network Interface Card, Bridges, Layer 2 Switches
Physical	Hub, Repeater, cabling

1. Briefly, explain each layer of OSI model

The specific description for each layer is as follows:

Layer 7: Application Layer
Defines interface to user processes for communication and data transfer in network
Provides standardized services such as virtual terminal, file and job transfer and operations

Layer 6: Presentation Layer
Masks the differences of data formats between dissimilar systems
Specifies architecture-independent data transfer format
Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Layer 5: Session Layer
Manages user sessions and dialogues
Controls establishment and termination of logic links between users
Reports upper layer errors

Layer 4: Transport Layer
Manages end-to-end message delivery in network
Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
Provides connectionless oriented packet delivery

Layer 3: Network Layer
Determines how data are transferred between network devices
Routes packets according to unique network device addresses
Provides flow and congestion control to prevent network resource depletion

Layer 2: Data Link Layer
Defines procedures for operating the communication links
Frames packets
Detects and corrects packets transmit errors

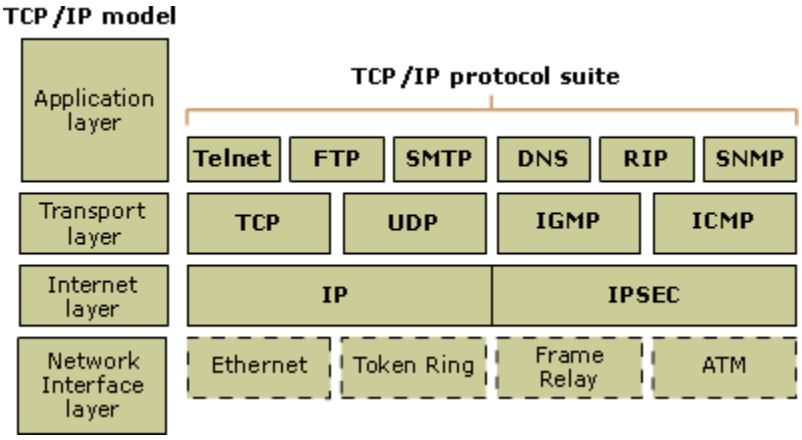
Layer 1: Physical Layer
Defines physical means of sending data over network devices
Interfaces between network medium and devices
Defines optical, electrical and mechanical characteristics

2. Briefly, explain each layer of TCT/IP model

The TCP/IP model

TCP/IP is based on a four-layer reference model. All protocols that belong to the TCP/IP protocol suite are located in the top three layers of this model.

As shown in the following illustration, each layer of the TCP/IP model corresponds to one or more layers of the seven-layer Open Systems Interconnection (OSI) reference model proposed by the International Standards Organization (ISO).



The types of services performed and protocols used at each layer within the TCP/IP model are described in more detail in the following table.

Layer	Description	Protocols
Application	Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols
Transport	Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data.	TCP, UDP, RTP
Internet	Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams.	IP, ICMP, ARP, RARP
Network interface	Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

Frame Types

A frame type is the format of the packet that your Operating System will use to communicate over your network. Below is a table of the different types:

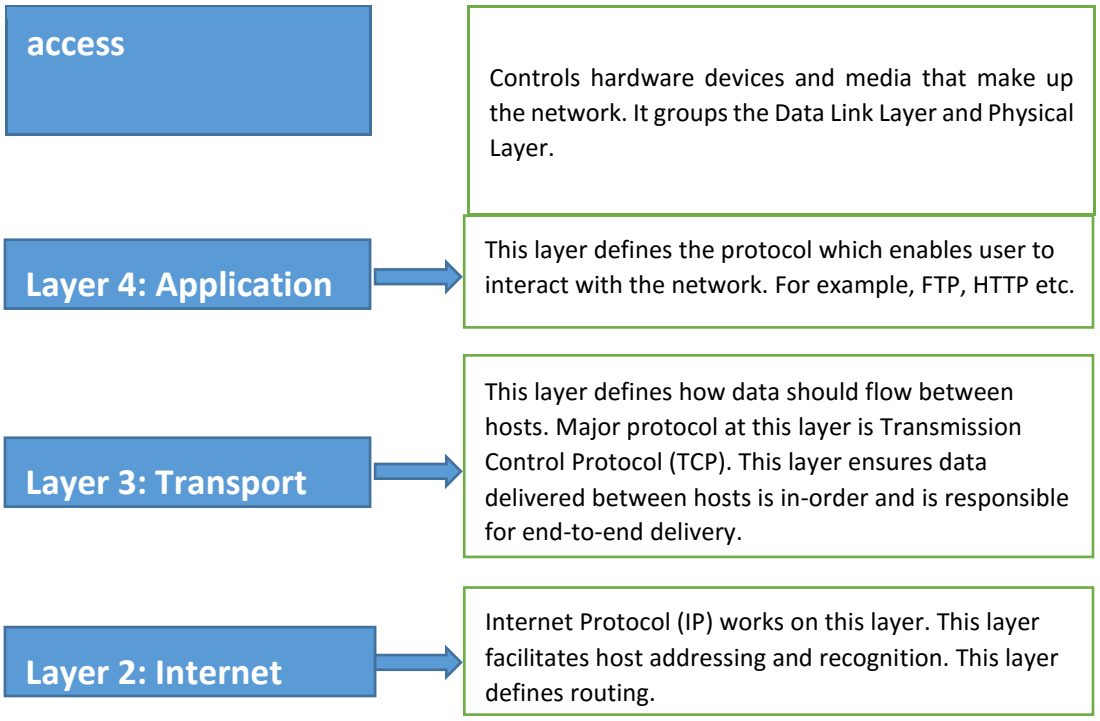
802.1	Internetworking

802.2	Logical link control - LLC adds header information that identifies the upper layer protocols sending the frame.
802.3	Ethernet - Media Access Control (MAC) sub-layer uses Carrier Sense Multiple Access with Collision Detection(CSMA/CD)
802.4	Token bus LAN
802.5	Token Ring BUS
802.6	Metropolitan Area network (MAN)
802.7	Broadband
802.8	Fiber optic
802.9	Integrated voice/Data
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority. Like 100VG-Any LAN

2.7 TCP/IP model

2.7.1 Introduction

The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model. TCP/IP model is the combination of TCP as well as IP models. This model ensures that data received is same as the data sent, and the data bytes are received in sequence. This model mainly defines how data should be sent (by sender) and received (by receiver). Most common examples of applications using this model include the email, media streaming, or World Wide Web (WWW). Presentation and session layers OSI model are not there in TCP/IP model. TCP/IP model comprises 4 layers that are as follows:



98

1. Application Layer

Application layer is the top most layer of four layers TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

It groups the functions of OSI Application, Presentation and Session Layers. It includes protocols like:

- The Hypertext Transfer Protocol (HTTP) is used to transfer files that make up the Web pages of the World Wide Web.
- The File Transfer Protocol (FTP) is used for interactive file transfer.
- The Simple Mail Transfer Protocol (SMTP) is used for the transfer of mail messages and attachments.
- Telnet, a terminal emulation protocol, is used for logging on remotely to network hosts.

1. **Transport layer**

Transport Layer (also known as the Host-to-Host Transport layer) is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data. It is responsible for providing the Application layer with session and datagram communication services.

The core protocols of the Transport layer are Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

- TCP provides a one-to-one, connection-oriented, reliable communications service. TCP is responsible for the establishment of a TCP connection, the sequencing and acknowledgment of packets sent, and the recovery of packets lost during transmission.
- UDP provides a one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used when the amount of data to be transferred is small (such as the data that would fit into a single packet).

The Transport layer encompasses the responsibilities of the OSI Transport layer and some of the responsibilities of the OSI Session layer.

3. Internet layer

The Internet layer is responsible for addressing, packaging, and routing functions. The core protocols of the Internet layer are IP, ARP, ICMP, and IGMP.

- The Internet Protocol (IP) is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets.
- The Address Resolution Protocol (ARP) is responsible for the resolution of the Internet layer address to the Network Interface layer address such as a hardware address.
- The Internet Control Message Protocol (ICMP) is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets.
- The Internet Group Management Protocol (IGMP) is responsible for the management of IP multicast groups.

The Internet layer is analogous to the Network layer of the OSI model.

4. Network Access Layer

This layer basically controls hardware devices and media that make up the network. Its tasks include routing of data, sending it over the network, verifying the data format, and converting the signs from analog to the digital format. TCP/IP can be used to connect differing network types. These include LAN technologies such as Ethernet and Token Ring and WAN technologies such as X.25 and Frame Relay.

The Network Interface layer encompasses the Data Link and Physical layers of the OSI model.

1.7.2 Summary of network models

The 2 network models do realize the same job of sending data between different networks. By comparing OSI and TCP/IP models, there is a difference because the number of layers differs. However, some layers like application in TCP/IP do the job done by many layers in OSI models. For example Application layer and Network layer in TCP/IP combine the role of many layers.

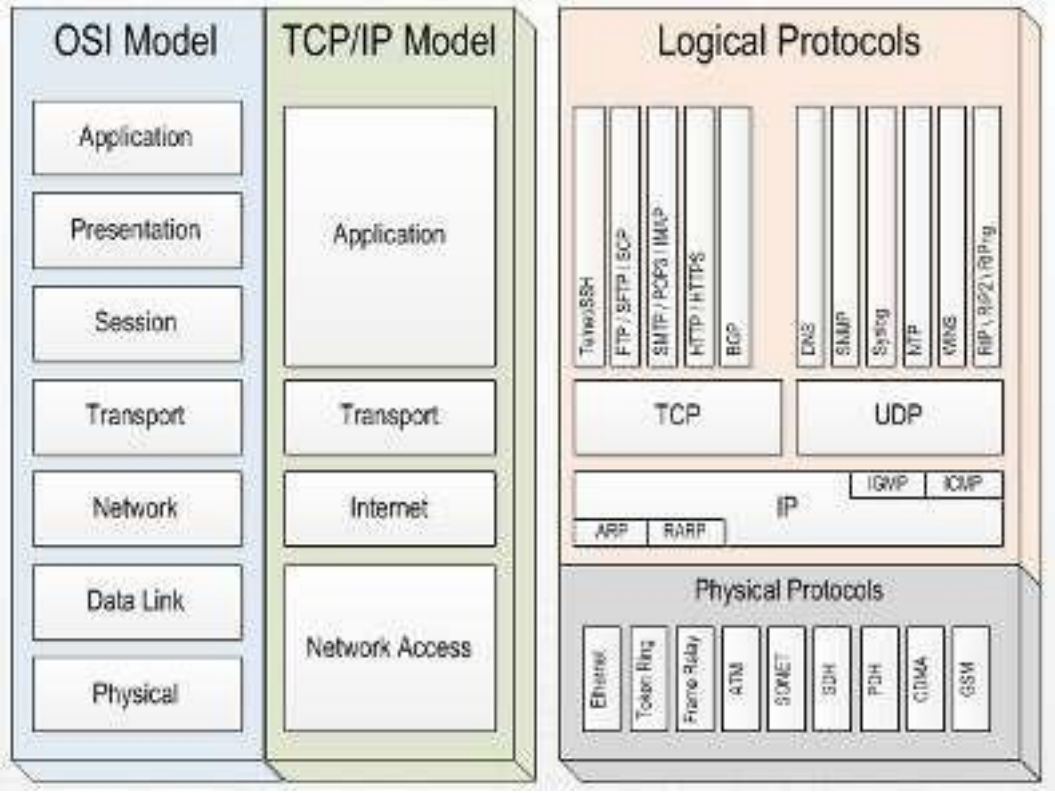


Figure 2.66: Network models

Table 2. 6: OSI vs. TCP/IP models

Sr. No.	TCP/IP Reference Model	OSI Reference Model

1	Defined after the advent of Internet.	Defined before advent of Internet.
2	Service interface and protocols were not clearly distinguished before	Service interface and protocols are clearly distinguished
3	TCP/IP offers support for connectionless communication within	In the network layer, OSI supports both connectionless and connection-oriented
4	TCP/IP supports Internet working	Internet working not supported
5	Loosely layered	Strict layering
6	Protocol Dependent standard	Protocol independent standard
7	More Credible	Less Credible
8	TCP reliably delivers packets, IP does not reliably deliver packets	All packets are reliably delivered

Application activity 2.7:

1. Which of the following are layers in the TCP/IP model? (Choose three.)

   a. Application
   b. Session
   c. Transport
   d. Internet
   e. Data Link
   f. Physical

2. What layer in the TCP/IP stack is equivalent to the Transport layer of the OSI model?

   a. Application
   b. Host-to-Host
   c. Internet
   d. Network Access

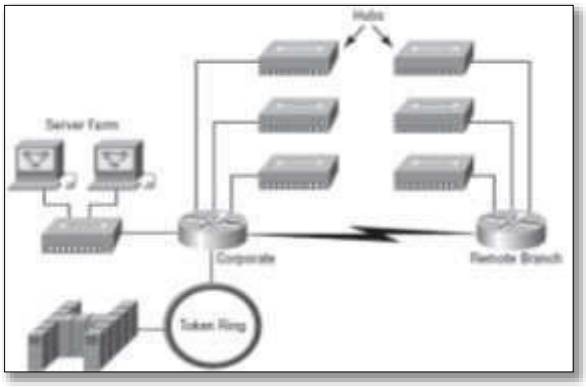
3. Using a figure, describe TCP/IP and OSI network models with their associated protocols.
4. Describe the purpose and basic operation of the protocols in the OSI and TCP models.

2.8 Network switching

Learning activity 2.8:

Look at the following two network designs represented by figure A and B and answer questions:

1. Describe what you see.
2. What is the difference between these two designs?



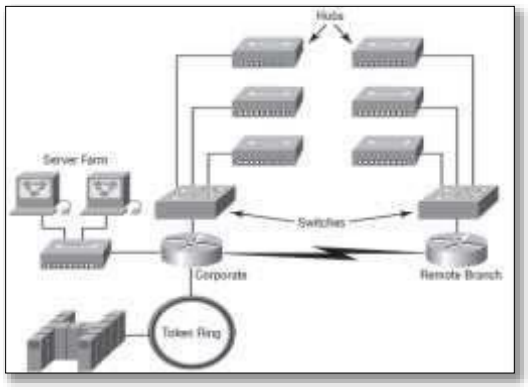


Figure 2.67: A *Figure 2.68: B*

I I.2 Comparison between TCP/IP and OSI Model

There is no direct correlation between the TCP protocol model and the OSI Model, but they are roughly equivalent in the services provided. The following diagram shows a comparison between the models:

Similarities

The main similarities between the two models include the following:

-Both models have (inter)network, transport and Application layers, though other layers are different.

- They share similar architecture. Both of the models share a similar architecture. This can be illustrated by the fact that both of them are constructed with layers.

- They share a common application layer. Both of the models share a common "application layer". However in practice this layer includes different services depending upon each model.

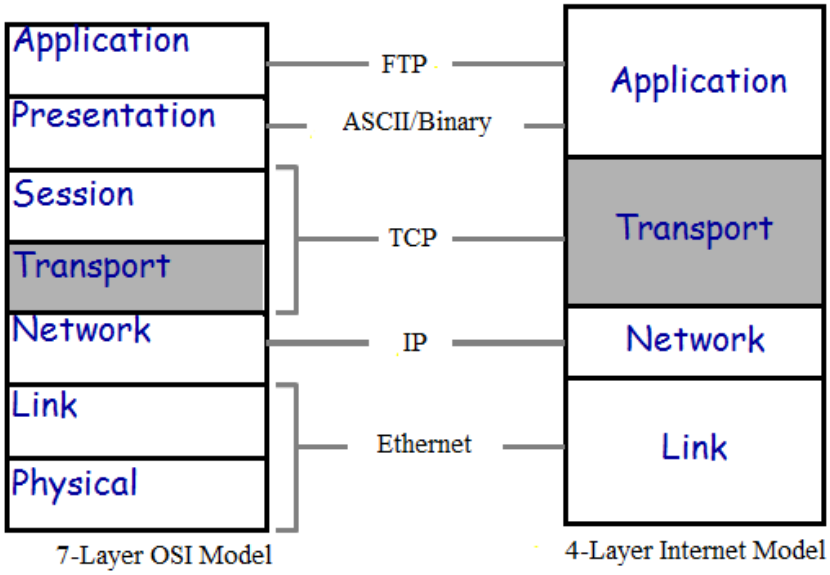
- Both models have comparable transport and network layers. This can be illustrated by the fact that whatever functions are performed between the presentation and network layer of the OSI model similar functions are performed at the Transport layer of the TCP/IP model.

- Knowledge of both models is required by networking professionals

- Both models assume that packets are switched. Basically this means that individual packets may take differing paths in order to reach the same destination.

Dissimilarities

1.Number of layers: The OSI model consists of 7 architectural layers whereas the TCP/IP only has 4 layers.



-TCP/IP combines the presentation and session layer issues into its application layer.

- TCP/IP combines the OSI data link and physical layers into the network access layer.

NO	OSI	TCP/IP
	The OSI model however is a "generic, protocol- independent standard."	TCP/IP Protocols are considered to be standards around which the internet has developed.
2	The OSI model originally distinguishes between service, interval and protocols.	The TCP/IP model doesn't Clearly distinguish between service, interval and protocol.
3	The OSI model is a reference model.	The TCP/IP model is an implementation of the OSI model.
4	In OSI model, the protocols came after the model was described. OSI emerged about 5 years after industry had adopted TCP/IP.	In TCP/TP model, the protocols came first, and the model was really just a description of the existing protocols.
5	The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection -oriented communication in transport layer.	The TCP/IP model supports both connectionless and connection-oriented communication in the transport layer., giving users the choice.

Connectionless and connection-oriented communication

The terms ***connection oriented*** and ***connectionless*** are descriptive words used to describe different kinds of communication.

CONNECTION ORIENTED

Connection-Oriented means that when devices communicate, they perform handshaking to set up an end-to-end connection. The handshaking process may be as simple as syncrhonization such as in the transport layer protocol TCP, or as complex as negotiating communications parameters as with a modem.

Connection-Oriented systems can only work in bi-directional communications environments. To negotiate a connection, both sides must be able to communicate with each other. This will not work in a unidirectional environment.

CONNECTIONLESS

Connectionless means that no effort is made to set up a dedicated end-to-end connection.

Connectionless communication is usually achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there, or if it is prepared to receive the information. When there is little interference, and plenty of speed available, these systems work fine. In environments where there is difficulty transmitting to the destination, information may have to be re-transmitted several times before the complete message is received.

Citizens Band radios is a good example of connectionless communication. You speak into the mike, and the radio transmitter sends out your signal. If the person receiving you doesn't understand you, there's nothing his radio can do to correct things, the receiver must send you a message back to repeat your last message.

IP, UDP, ICMP, DNS, TFTP and SNMP are examples of connectionless protocols in use on the Internet.

A Critique of the OSI Model and Protocols:

OSI did not take over the world because of four reasons namely: Bad timing, Bad technology, Bad implementations, bad politics.

1. Bad Timing:

Timings related factors that hindered OSI Model to be adopted in practice include:

. Widespread adoption of the TCP/IP protocols preceded the formalization of the OSI model.

. Vendors already begun offering TCP/IP based products.

. OSI emerged about 5 years after industry had adopted TCP/IP.

. Vendors were reticent to add support for a second protocol stack until momentum had gathered behind OSI.

.The combination of these factors meant that OSI was never adopted in practice.

Technology related factors which hindered OSI Model to be adopted in practice include:

. Some parts of the OSI model are fundamentally flawed.

. Although there are 7 layers, 2 of these (session, presentation) are almost empty and 2 others (data link, network) are cramped.

. Additionally some functions such as addressing, error control are recurring at each layer.

Implementations factor:

. Early implementations of OSI were inefficient, contrast withTCP/IP implementations which are easy to use, scalable and robust.

Politics factor:

. OSI was widely perceived as the product of quasi-government standards processes rather than driven by good design processes.

A Critique of the TCP/IP MODEL:

. Lack of distinction between concepts.

. Doesn't clearly distinguish between service, interface and protocol.

. Not adaptable – Not a general model and hence poorly adapted to other protocol Stacks.

. Ambiguous layers – Host-to-network is not really a layer, but an interface between network and data link layers.

. Omitted layers – Physical and data link layers are not present.

. Early implementations were fragile.

2.8.1 Definition

Switching is a process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called **ingress**, and when data leaves a port or goes out it is called **egress**.

A switched network consists of a series of interlinked nodes, called switches. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing. The Figure below shows a switched network.

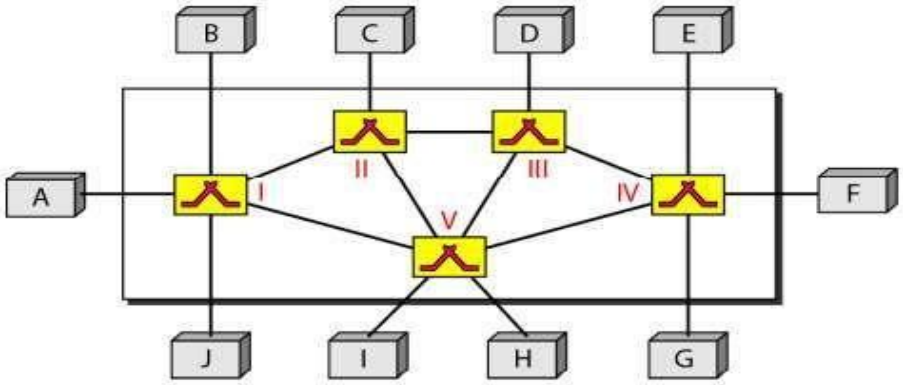


Figure 2.69: Switched network

The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

The advantages of switches are as follows:

- Switches increase available network bandwidth
- Switches reduce the workload on individual computers
- Switches increase network performance
- Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called micro segmentation)
  - Switches connect directly to workstations.

2.8.2 Switching methods

The classification of switched networks is given by the figure below.

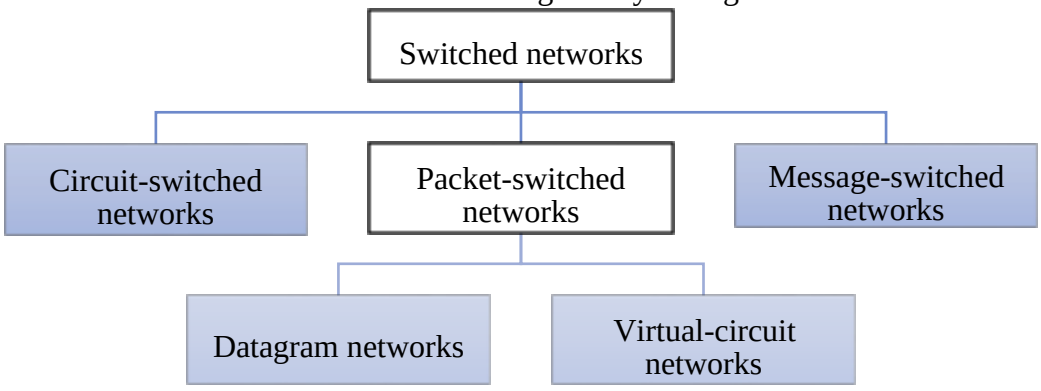


Figure 2.70: Classification of switched networks

2.8.2.1 Circuit-Switched Networks

Circuit switching is a switching method in which a dedicated communication path in physical form between two stations within a network is established, maintained and terminated for each communication session. Applications which use circuit switching may have to go through three phases:

- Establish a circuit
- Transfer the data
- Disconnect the circuit

2.8.2.2 Packet Switched Networks

In **packet switched** data networks all data to be transmitted is first broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

It is easier for intermediate networking devices to store small size packets and they do not take much resources either on carrier path or in the internal memory of switches.

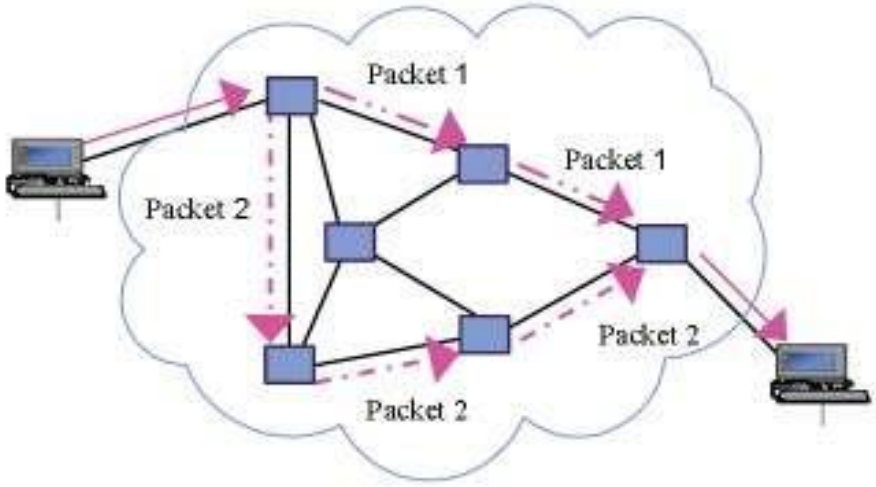


Figure 2.71: Packets sent over the network

Packet switching can be done through the following technologies:

a) **Datagram networks**

Packets are treated independently and may take different routes. Datagram is better if numbers of packets are not very large.

b) **Virtual circuit networks**

In virtual circuit, a logical path is setup prior the transmission and therefore, no routing decision is to make which ensure that packet are forwarded more quickly than datagram. The logical path between destination and source also assure the sequencing of packet and better error control. However, virtual circuit is less reliable because Interruption in a switching node loses all circuit through that node.

2.8.2.3 Message switching

In message switching, if a station wishes to send a message to another station, it first adds the destination address to the message. Message switching does not establish a dedicated path between the two communicating devices *i.e.* no direct link is established between sender and receiver. Each message is treated as an independent unit.

Consider a connection between the users (A and D) in the figure below (i.e. A and D) is represented by a series of links (AB, BC, and CD).

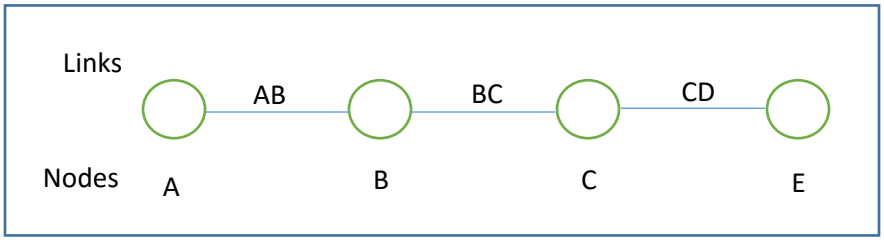


Figure 2.72: A connection between A and D

For example, when an email message is sent from A to D, it first passes over a local connection (AB). It is then passed at some later time to C (via link BC), and from there to the destination (via link CD). At each message switch, the received message is stored, and a connection is subsequently made to deliver the message to the neighboring message switch.

Application activity 2.8

1. How does the message switching differ from circuit switching?
2. Explain the technologies used in packet switching.

END UNIT ASSESSMENT ACTIVITIES

1. Your school has acquired 60 computers from the Rwanda Education Board (REB) and wishes to distribute them as follows:

- Administration: 3 computers
- Staff room: 7 computers
- Computer lab for students in Ordinary level: 30 computers
- Computer lab for students in Advanced level: 20 computers

a) List and describe specifications of all materials needed to setup 2 wireless LANs within the school.
b) Is it possible to secure those wireless networks?
c) Indicate the type of wireless security to be used.

2. Discuss the advantages of Fiber optic cables within a LAN.
3. Why routers and switches do not operate at the same OSI reference model layer?
4. What are the common steps in configuring both wireless router and access points?
5. Is it possible to change the default gateway of your computer? Explain.
6. When and how both public and private IP addresses are used within the same network?
7. Describe the purpose and basic operation of the protocols in the OSI and TCP models.
8. What are the advantages of using OSI layered model?
9. Discuss the importance of switches within a LAN.

LEARNING OUTCOME 2.2: DESCRIBE NETWORK STANDARDS

- Importance of standards
- Internet standards
- Types of standards

De Facto standards

De Jure standards

- Standards organizations

ISO

IEEE

ANSI

ITU-Formally CCITT

EIA

Telcodia

DESCRIBE NETWORK STANDARDS

1.DEFINITION

Having recognized excellence or authority

Falling within an accepted range of size,amount,power,quality,of usable or serviceable grade or quality,etc

2. Importance of standard

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers in guaranteeing national and international interoperability of data and telecommunications technology and processes.

Networking Standards. Networking standards ensure the interoperability of networking technologies by defining the rules of communication among networked devices. Networking standards exist to help ensure products of different vendors are able to work together in a network without risk of incompatibility.

3. Internet standards

In computer network engineering, an **Internet Standard** is a normative specification of a technology or methodology applicable to the **Internet**. **Internet Standards** are created and published by the **Internet** Engineering Task Force (IETF).

All **Internet standards** and many other Internet specifications are documented in a series of documents called Request for Comments or RFCs

An Internet Standard is characterized by a high degree of technical maturity and by a generally held belief that the specified protocol or service provides significant benefit to the Internet community. Generally Internet Standards cover interoperability of systems on the Internet through defining protocols, message formats, schemas, and languages. The most fundamental of the Internet Standards are the ones defining the Internet Protocol.

An Internet Standard ensures that hardware and software produced by different vendors can work together. Having a standard makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time. Normally, the standards used in data communication are called protocols.

Network Standards

The standards are the documents that contain technical and physical specifications about the network being designed.

Networking standards define the rules for data communications that are needed for interoperability of networking technologies and processes. Standards help in creating and maintaining open markets and allow different vendors to compete on the basis of the quality of their products while being compatible with existing market products.

During data communication, a number of standards may be used simultaneously at the different layers. The commonly used standards at each layer are:

1. **Application layer :** HTTP, HTML, POP, H.323, IMAP
2. **Transport layer:** TCP, SPX
3. **Network layer:** IP, IPX
4. **Data link layer:** Ethernet IEEE 802.3, X.25, Frame Relay
5. **Physical layer:** RS-232C (cable), V.92 (modem)

4.Types of standards

Standards are of two types

1. **De facto:** These are the standards that are followed without any formal plan or approval by any organization. They have come into existence due to traditions or facts. For example, the HTTP had started as a de facto standard.

   De facto means by tradition or by facts. These standards are developed without any formal planning. These standards come into existence due to historical developments. These standards are still being used by many organizations in the world. SNA is an example of de facto standard

SNA: Systems Network Architecture is an IBM networking architecture that dates back to the 1970s, when mainframe computers roamed the earth and PCs had barely emerged from the primordial computer soup.

SNA was designed primarily to support huge terminals such as airline reservation and banking systems, with tens of thousands of terminals attached to central host computers. Now that IBM mainframes support TCP/IP and terminal systems have all but vanished, SNA is beginning to fade away. Still, many networks that incorporate mainframe computers have to contend with SNA.

2. **De jure:** These standards are the ones which have been adopted through legislation by any officially recognized standards organization. Most of the communication standards that are used today are de jure standards.

De jure means according to law or regulation. These standards are developed with proper research to fulfill the requirement of data communication.

Most standards are voluntary in the sense that they are offered for adoption by people or industry without being mandated in law. Some standards become mandatory when they are adopted by regulators as legal requirements in particular domains.

The term *formal standard* refers specifically to a specification that has been approved by a standards setting organization. The term *de jure standard* refers to a standard mandated by legal requirements or refers generally to any formal standard. In contrast, the term *de facto standard* refers to a specification (or protocol or technology) that has achieved widespread use and acceptance – often without being approved by any standards organization (or receiving such approval only after it already has achieved widespread use). Examples of de facto standards that were not approved by any standards organizations (or at least not approved until after they were in widespread *de facto* use) include the Hayes command set developed by Hayes, Apple's TrueType font design and the PCL protocol used by Hewlett-Packard in the computer printers they produced.

5.Standards organizations

A standards organization, sometimes referred to as a standards body, is an organization with authority to endorse official standards for given applications.

A **standards organization**, **standards body**, **standards developing organization** (**SDO**), or **standards setting organization** (**SSO**) is an organization whose primary activities are developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise producing technical standards[1] that are intended to address the needs of a group of affected adopters.

Examples of standards organizations include:

- ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States.
- The IEEE (Institute of Electrical and Electronics Engineers) fosters the development of standards that often become national and international standards.
- The BSI (British Standards Institution) is a service organization that produces standards across a wide variety of industry sectors.

- The IETF (Internet Engineering Task Force) is the body that defines standard Internet operating protocols such as TCP/IP.
- OASIS (Organization for the Advancement of Structured Information Standards) exists to promote product-independent standards for information formats such as XML and HTML.

Standards that are endorsed by these and similar organizations are known as de jure standards. De facto standards, on the other hand, are technologies, products or methods that are very widely used although they have no official standing.

ITU: The International Telecommunication Union

The ITU has created numerous telecommunications standards including telegraph specifications, allocation of telephone numbers, interference protection, and protocols for a variety of communications technologies. The standards that are created through standards organizations lead to improved product quality, ensured interoperability of competitors' products, and they provide a technological baseline for future research and product development.

Some of the noted standards organizations are

1. International Standards Organization (ISO)
2. International Telecommunication Union (ITU)
3. Institute of Electronics and Electrical Engineers (IEEE)
4. American National Standards Institute (ANSI)
5. Internet Research Task Force (IETF)
6. Electronic Industries Association (EIA)

STANDARDS ORGANIZATIONS FOR DATA COMMUNICATION

An association of organizations, governments, manufacturers and users form the standards organizations and are responsible for developing, coordinating and maintaining the standards. The intent is that all data communications equipment manufacturers and users comply with these standards. The primary standards organizations for data communication are:

1. International Standard Organization (ISO) 79:

ISO 79 is the international organization for standardization on a wide range of subjects. It is comprised mainly of members from the standards committee of various governments throughout the world. It is even responsible for developing models which provides high level of system compatibility, quality enhancement, improved productivity and reduced costs. The ISO is also responsible for endorsing and coordinating the work of the other standards organizations.

2. International Telecommunications Union-Telecommunication Sector (ITU-T) 34:

ITU-T 34 is one of the four permanent parts of the International Telecommunications Union based in Geneva, Switzerland. It has developed three sets of specifications: the V series for modem interfacing and data transmission over telephone lines, the X series for data transmission over public digital networks, email and directory services; the I and Q series for Integrated Services Digital Network (ISDN) and its extension Broadband ISDN. ITU-T membership consists of government authorities and representatives from many countries and it is the present standards organization for the United Nations

3. Institute of Electrical and Electronics Engineers (IEEE) 40:

IEEE 40 is an international professional organization founded in United States and is compromised of electronics, computer and communications engineers. It is currently the world's largest professional society with over 200,000 members. It develops communication and information processing standards with the underlying goal of advancing theory, creativity, and product quality in any field related to electrical engineering.

##4. American National Standards Institute (ANSI) 16:

ANSI 16 is the official standards agency for the United States and is the U.S voting representative for the ISO. ANSI is a completely private, non-profit organization comprised of equipment manufacturers and users of data processing equipment and services. ANSI membership is comprised of people form professional societies, industry associations, governmental and regulatory bodies, and consumer goods.

##5. Electronics Industry Association (EIA) 24:

EIA [24] is a non-profit U.S. trade association that establishes and recommends industrial standards. EIA activities include standards development, increasing public awareness, and lobbying and it is responsible for developing the RS (recommended standard) series of standards for data and communications.

##6. Telecommunications Industry Association (TIA) [22]:

TIA [22] is the leading trade association in the communications and information technology industry. It facilitates business development opportunities through market development, trade promotion, trade shows, and standards development. It represents manufacturers of communications and information technology products and also facilitates the convergence of new communications networks.

##7. Internet Architecture Board (IAB) [13]:

IAB [13] earlier known as Internet Activities Board is a committee created by ARPA (Advanced Research Projects Agency) so as to analyze the activities of ARPANET whose purpose is to accelerate the advancement of technologies useful for U.S military. IAB is a technical advisory group of the Internet Society.

##8. Internet Engineering Task Force (IETF) [14]:

The **IETF** [14] is a large international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and smooth operation of the Internet.

##9. Internet Research Task Force (IRTF) [17]:

The **IRTF** [17] promotes research of importance to the evolution of the future Internet by creating focused, long-term and small research groups working on topics related to Internet protocols, applications, architecture and technology.

10.Telcordia

Telcordia (Bellcore) Testing **Standards**
ESPEC specializes in temperature and humidity test chambers that are needed to do the required tests of **Telcordia** Generic Requirements (GR) for reliability of telecommunications equipment. Platinous series models can fit many tests that you may be required to do. We also have many small benchtop chambers that are suitable for some of these tests, saving space and money.

Telcordia Telecommunications, now owned by telecommunications and information technology leader Ericcson, formatted a series of generic vendor-neutral standards for generic criteria for telecommunications equipment,

systems, or services. Industry actors are encouraged to continue contributing to these standards at Telcordia's 2015 Technical Forum

This document contains generic criteria for passive optical components to help promote the satisfactory operation of such components in network operator's single-mode fiber transmission networks and to permit economical planning and engineering.

GR-1221, Issue 3, presents the Telcordia view of proposed generic reliability assurance requirements for passive optical components, and is directed toward an equipment supplier's design engineering, manufacturing, procurement, and reliability/quality organizations. Common forms of passive fiber optic branching components include splitters, couplers, and wavelength division multiplexers (WDM-MUXES) and demultiplexers (WDM-DEMUXES).

Testing For

Passive Fiber Optic Components

Outdoor Network Interface Devices

Telcordia Electronic Reliability Prediction

The Telcordia Software Module of ITEM ToolKit calculates the reliability prediction of electronic equipment based on the Telcordia (Bellcore) TR-332 and SR-332 standards. These standards use a series of models for various categories of electronic, electrical and electro-mechanical components to predict steady-state failure rates which environmental conditions, quality levels, electrical stress conditions and various other parameters affect. It provides predictions at the component level, system level or project level for COTS (Commercial Off-The-Shelf Parts). The models allow reliability prediction to be performed using three methods for predicting product reliability:

Method I: Parts Count

Method II: Combines Method I predictions with laboratory data

Method III: Predictions based on field data

The Telcordia standard also documents a recommended method for predicting serial system hardware reliability. It contains instructions for suppliers to follow when providing predictions of their device, unit, or serial system reliability. It can also be used directly by telecommunications service providers for product reliability evaluation.

Device and unit failure rate predictions generated using this procedure are applicable for commercial electronic products whose physical design, manufacture, installation, and reliability assurance practices meet the appropriate Telcordia (or equivalent) generic and product-specific requirements.

Learning Outcome 2. 3: Identify and apply Network media and connectors

- Introduction to network media
- Types of media

Logical (wireless)

Physical Coaxial

♣ Thinnet

♣ Thicknet Twisted pair

♣ UTP, STP, FSTP Fiber optic

♣ Single mode fiber

♣ Multimode fiber

Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fiber cables used in wired networks, and radio waves used in wireless data communications networks.

Network Transmission Medium

This is the physical mean of communication between network computers.

Data transmission media are the physical materials used to transmit data between computers. Packet of data can be transmitted on network as **electrical signals** in **electric wire**, **light signal** in fiber optic cables or as **electromagnetic waves** through space.

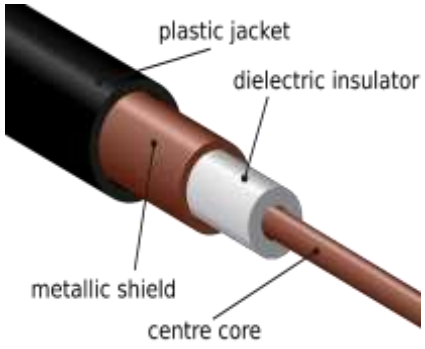
There are two main types of data communication media used in network:

1. **Bounded or Guided media:** which transmit signals by sending electricity or light over a cable wire. Common examples of bounded media are twisted cables, Coaxial cables and fiber optic cables.
2. **Unbounded media**: which transmit data through the air, radio waves, layer or infrared signal and satellite based microwaves, etc.

3.6.1 Guided transmission media

A wide variety of networking cables are **Coaxial, Fiber optic** and **twisted-pair** cables which use electrical signals over copper to transmit data while Fiber-optic cables use light signals to transmit data. These cables differ in bandwidth, size, and cost.

a. Coaxial cable



Picture 3. 19: Coaxial cable parts

It is used by both cable television companies and satellite communication systems and it carries data in the form of electrical signals. There are several types of coaxial cable:

- **Thicknet or 10BASE5** - used in networks and operated at 10 Mb/s with a maximum length of 1640.4 ft. (500 m.)
- **Thinnet 10BASE2** - used in networks and operated at 10 Mb/s with a maximum length of 607 ft. (185 m.)

b.Twisted-pair copper cabling

Twisted-pair is a type of copper cabling used for telephone communications and most Ethernet networks. The pair is twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs of wires in the cable.

The use of this cable is limited by two factors:

a) **Attenuation:** the strength of signal reduces as the distance increases i.e the cables loose signals strength when they exceed their maximum length stated in network specification.

There exist three main sources of attenuation:

- Resistance or impedance: this refers to the loss resulting from the wire resistance. The loss is minimized with the choice of the metal with low resistivity (copper and Gold for example)
- **Dielectric losses:** are caused by the heating effects when a varying electric field passes through an insulator
- **Radiation losses:** occurs because the cable acts as an antenna. All these losses increase with frequency.

b). Crosstalk: this refers to interference generated by cables when they are too close to each other.

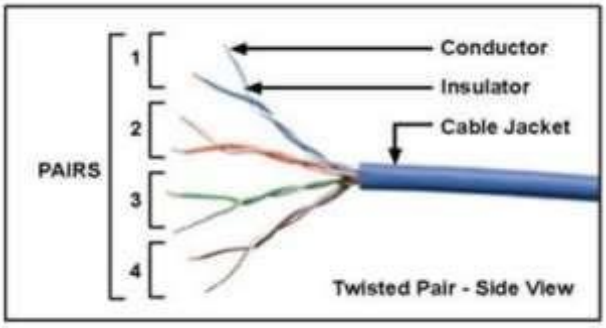
Signals from one line get mixed with signals from another.

3.6.2. Types of twisted pair cables

There are two types of twisted pair cables: unshielded and shielded cables

a. Unshielded twisted-pair (UTP)

Unshielded twisted-pair (UTP) cabling is the most common variety of twisted-pair cabling.

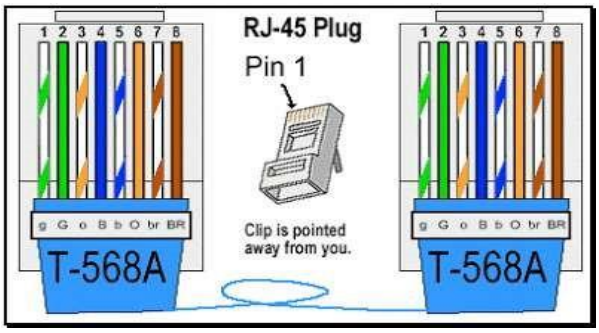


Picture 3. 20: Unshielded twisted pair

As shown in the above Figure, UTP cable consists of four pairs of color-coded wires that have been twisted together and then encased in a flexible plastic sheath that protects from minor physical damage. The twisting of wires helps protect against crosstalk. However, UTP does not protect against electromagnetic interference (EMI) or radio frequency interference (RFI). EMI and RFI can be caused by a variety of sources including electric motors and fluorescent lights.

There are two different wiring schemes called T568A and T568B. Using the T568A and T568B wiring schemes, two types of cables can be created: a **straight-through** cable and a **crossover cable.**

1. **A straight-through cable** is the most common cable type. It maps a wire to the same pins on both ends of the cable. The order of connections (the pin out) for each color is the exact same on both ends.



Picture 3. 21: Wiring Schemes T568A

Two devices directly connected and using different pins for Transmit and Receive are known as unlike devices. They require a straight-through cable to exchange data. For example, connecting a PC to a switch requires a straight-through cable.

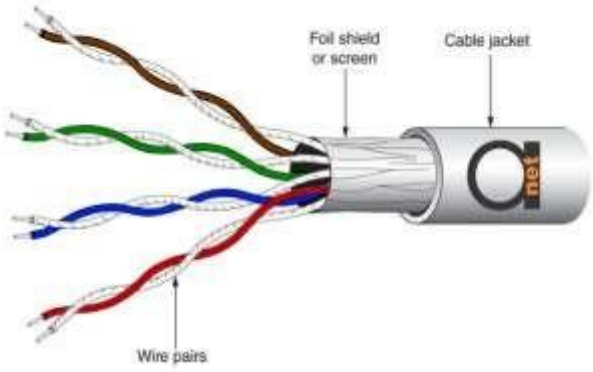
2. **A crossover cable** uses both wiring schemes. T568A on one end of the cable and T568B on the other end of the same cable.

Devices that are directly connected and use the same pins for transmit and receive, are known as like devices. They require the use of a crossover cable to exchange data. For example, connecting a PC to another PC requires a crossover cable.

Note: The most used cable standards are below:

- 100Base-TX: known as Fast Ethernet, it uses category 5, 5E, or 6 UTP cable and it wires u to 100 meters long.
- 1000Base-T means that the speed of the network is up to 1000 Mbps, baseband signaling is sed, T stands for twisted-pair as UTP cable used

3.6.2. Shielded twisted-pair (STP)



The STP type similar to UTP cable except that there is a metal foil or braided metal-mesh cover that encases each pair of insulated wires. The extra covering in shielded twisted pair wiring protect the transmission line from electromagnetic interference (EMI) leaking into or out of cable. However this can make cables quite bulky and harder to install.

The basic **difference between UTP** and STP is that **UTP** is a cable with wires that are **twisted** together to reduce noise and crosstalk. On other hand, STP is a **twisted pair** cable confined in foil or mesh shield that guards the cable against electromagnetic interference.

APPLICATION ACTIVITY 3.10

Requirement:

1. Unshielded twisted pair (UTP) patch cable
2. Modular connector (8P8C plug, aka RJ45)
3. Crimping tool
4. Cable tester (optional, but recommended

Step 1: Strip the cable jacket about 1.5 inch down from the end.

Step 2: Spread the four pairs of twisted wire apart.

Step 3: Untwist the wire pairs and neatly align them in the T568B orientation.

Step 4: Cut the wires as straight as possible, about 0.5 inch above the end of the jacket.

Step 5: Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.

Step 6: Push the connector inside the crimping tool and squeeze the crimper all the way down.

Step 7: Repeat steps 1-6 for the other end of the cable.

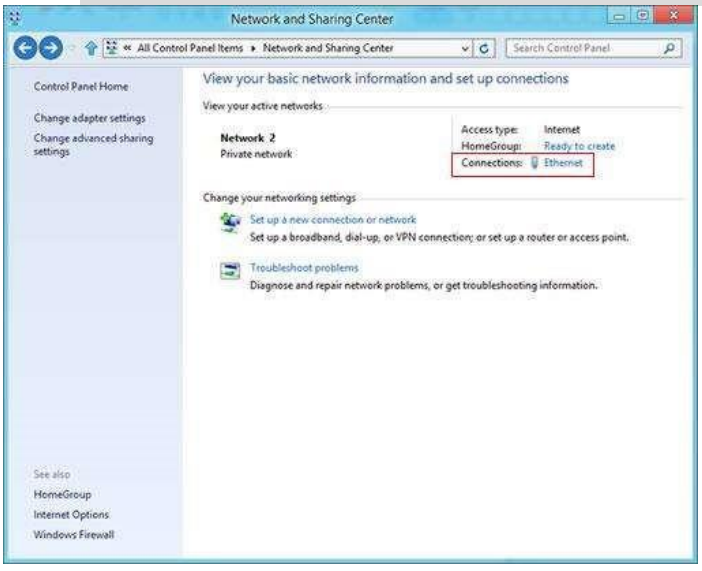
Step 8: To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.

APPLICATION ACTIVITY 3.11

Step 1: Open the Network and Sharing Center:

Step 2: Select the Control Panel from the Start menu.

Step 3: Select Open Network and Sharing Center and click Network and Sharing Center.



3. Fiber optic cables

An optical fiber cable, also known as a fiber optic cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light signals **Advantages of fiber optic**

(a) Since they transmit light rather than electronic signal, the problem of electrical interference is eliminated , therefore they are not affected by radio interference or cross talk

(b) They have become the standard for connecting networks between buildings due to their immunity the effects of moisture and lighting.

(c) Fiber optic can transmit signal over much longer distance than coaxial cable and twisted cables

(d) They can carry information at high rate speed between

(e) The distance can be up to 2000 meters without repeater

(f) Security: it is difficult to tap into optical fiber line. If this is happen it will be noticed immediately.

(g) Low transmission loss

(h) Data can be transmitted digitally

(i) They are more resistant to adverse weather conditions.

Network Cabling /data transmission media

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The types of cables used in networks:

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable

- Coaxial Cable
- Fiber Optic Cable

4.1 Twisted Pair cable

- Uses copper wire similar to those used for home and office telephone connections. Twisting the wire help to reduce electrical interference.
- The twisted pair cable is used to connect the computers in a star arrangement
- The twisted pair cable consists of thin wire twisted around each other.
- Twisted pair cable comes is various grades called categories
- Rj45 connectors are used to connect the twisted pair cables
- The maximum allowable cable length between the hub and the computer is 100 meters.

Twisted pair cable

Advantages of twisted pair cable

- Least expensive
- Easy to install **Disadvantages**

- Only one signal can be sent or received at a time.
- Limited capacity of spanning long distances, and for handling high speed transmission rates.

Twisted pair cable come in two forms:

- **STP – Shielded twisted pair**

- refers to the amount of insulation around the wire, therefore reducing noise.

- **UTP – Unshielded twisted pair**
  - cables mostly used by the telephone company.

Unshielded Twisted Pair (UTP) Cable

Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks.

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire.

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

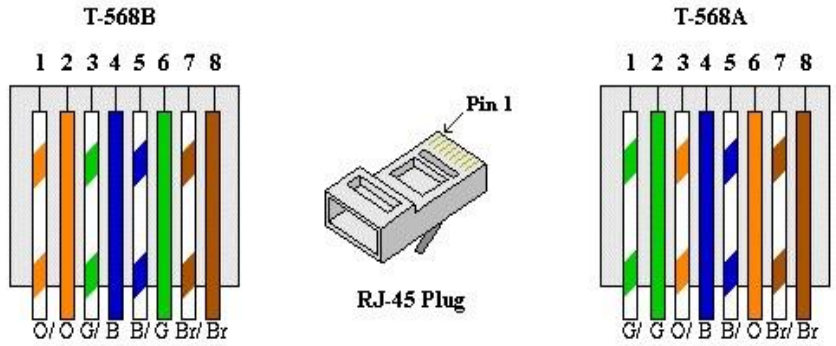
RJ-45 connector

Categories of Unshielded Twisted Pair

Category	Speed	Use
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Note:

There are two wiring standards for these cables, called T-568A and T568B. They differ only in pin assignments, not in uses of the various colors. The illustration bellow shows both standards. With the T-568B specification the orange and green pairs are located on pins 1, 2 and 3, 6 respectively.



The T-568A specification reverses the orange and green connections, so that the blue and orange pairs are on the center 4 pins, which makes it more compatible with the telco voice connections.

Shielded Twisted Pair (STP) Cable

- Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.).
- If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may

be the solution. Shielded cables can also help to extend the maximum distance of the cables.

- Shielded twisted pair cable is available in three different configurations:
- Each pair of wires is individually shielded
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

4.2.Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from outside.

Coaxial cable

Coaxial cables Support two types of transmissions

- **Base band networks:** - Single channels, links limited in length. Appropriate for small to medium sized office
- **Broad bound cable:** - Identical to the network medium used for television. This type of network supports multi channel transmission, in which up to 30 different signals can travel, including data voice and video signals.

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable.

The two types of coaxial :

Thin coaxial cable is also referred to as **thinnet** or **BNC** cable because of the connector used at the end of the cable. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being **200 meters**. In actual fact the maximum segment length is 185 meters.

The coaxial cable is used in connecting the bus topology. At each computer, a T connector is used to connect two cables to the network interface card.

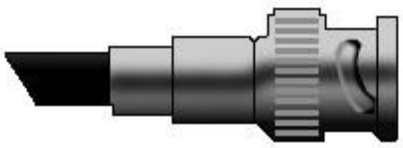
Thick coaxial cable is also referred to as **thicknet**. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being **500 meters**. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network.

- This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend (coude) easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the BayoneNeill-Concelman (BNC) connector. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the

BNC connectors that crimp rather screw, into the cables



BNC connector

4.3.Fiber Optic Cable

- Fiber optic cabling consists of a center glass core surrounded by several layersof protective materials . It transmits light rather than electronic signals eliminating the problem of electrical interference.
- This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture (humidite)and lighting(eclairage).

Fiber optic cable

- Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services.
- The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

➢ Facts about fiber optic cables:

- Outer insulating jacket is made of Teflon or PVC.
- Kevlar fiber helps to strengthen the cable and prevent breakage.
- A plastic coating is used to cushion the fiber center.
- Center (core) is made of glass or plastic fibers.

- **There are two common types of fiber cables** -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

Metal connector for optic cable

Fiber optics has several advantages over other types of cables

- Fiber optic cables have a much greater bandwidth than metal cables. This means that they can carry more data.
- Fiber optic cables are less susceptible(probable) than metal cables to interference.
- Fiber optic cables are much thinner and lighter than metal wires.
- Data can be transmitted digitally rather than analogically.
- Fastest in transmitting data.
- Offers high degree of security from illegal tapping and total immunity from electrical interference
- Sends data over huge distances, at high speed

Disadvantages of Fiber optic

- Very Costly
- Difficult to install and to work with.

Ethernet Cable Summary

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber

1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

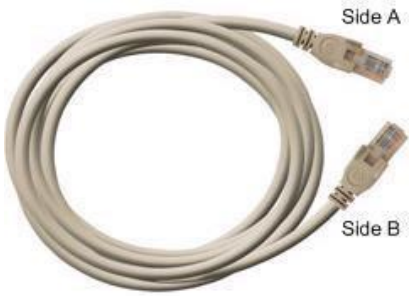
4.4.STRAIGHT AND CROSSOVER CABLE

Common Ethernet network cables are straight and crossover cable. This Ethernet network cable is made of 4 pair high performance cable that consists twisted pair conductors that used for data transmission. Both end of cable is called RJ45 connector.

The cable can be categorized as **Cat 5, Cat 5e, Cat 6 UTP cable**. Cat 5 UTP cable can support 10/100 Mbps Ethernet network, whereas Cat 5e and Cat 6 UTP cable can support Ethernet network running at 10/100/1000 Mbps. You might heard about Cat 3 UTP cable, it's not popular anymore since it can only support 10 Mbps Ethernet network.

Ethernet uses pins 1, 2, 3, and 6(for both crossover and straight cables).

Straight and crossover cable can be Cat3, Cat 5, Cat 5e or Cat 6 UTP cable, the only difference is each type will have different wire arrangement in the cable for serving different purposes.



4.4.1Straight Cable

You usually use straight cable to connect different type of devices. This type of cable will be used most of the time and can be used to:

1) Connect a computer to a switch/hub's normal port.

2) Connect a computer to a cable/DSL modem's LAN port.

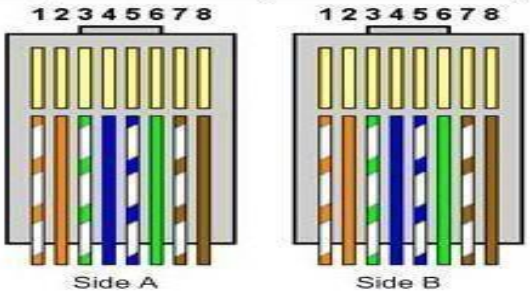
3) Connect a router's WAN port to a cable/DSL modem's LAN port.

4) Connect a router's LAN port to a switch/hub's port. (normally used for expanding network)

5) Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. **Both sides (**side A and side B**) of cable have wire arrangement with same color**.

Pin ID	Side A	Side B
1	Orange-white	Orange-white
2	Orange	Orange
3	Green-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Green	Green
7	Brown-white	Brown-white
8	Brown	Brown



4.4.2Crossover Cable

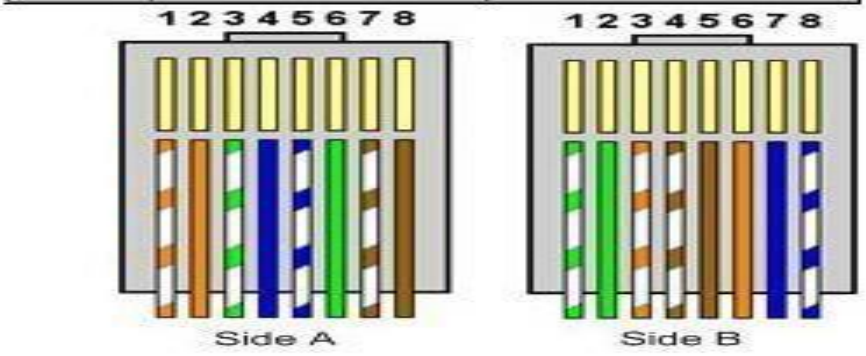
An **Ethernet crossover cable** is a type of Ethernet cable used to connect computing devices together directly where they would normally be connected via a network switch, hub or router, such as directly connecting two personal computers via their network adapters.

Briefly, a crossover cable is usually used to connect same type of devices. A crossover cable can be used to:

1) Connect 2 computers directly.
2) Connect a router's LAN port to a switch/hub's normal port. (normally used for expanding network)
3) Connect 2 switches/hubs by using normal port in both switches/hubs.

In you need to check how crossover cable looks like, **both side (**side A and side B**) of cable have wire arrangement with following different color**.

Pin ID	side A	side B
1	Orange-white	green-white
2	Orange	green
3	green-white	orange-white
4	blue	brown-white
5	blue-white	Brown
6	green	orange
7	brown-white	Blue
8	brown	blue-white



4.5.THE MAIN DIFFERENCE BETWEEN CROSSOVER AND STRAIGHT THROUGH

- Straight through cable
- If you hold the two ends of an RJ-45 cable side by side, you'll see eight colored strips, or pins, at each end.

- If the order of the colored pins is the same at each end, then the cable is straight through.
- If the order of the colors is reversed at each end, then the cable is crossed over or rolled.
- Straight-thru Ethernet uses pins 1, 2, 3, and 6.
- Straight-thru cables are used for switch to router cabling, switch to PC or server cabling, or hub to PC or server cabling.
- UTP Implementation Straight-through
- Crossover cable
- Ethernet uses pins 1, 2, 3, and 6. For crossover, pin 1 is connected to 3, and oin 2 is connected to 6.
- Crossover cables are used for switch to switch cabling, PC to PC cabling, switch to hub cabling, hub to hub cabling, or router to router cabling.

• Types of connectors

⎱ RJ45,RJ11 ⎱ BNC ⎱ USB ⎱ Firewire ⎱ VGA ⎱ Serial ⎱ BNC-T ⎱ F type

MT-RG ⎱ RS-232

ADVANTAGES OF MEDIA

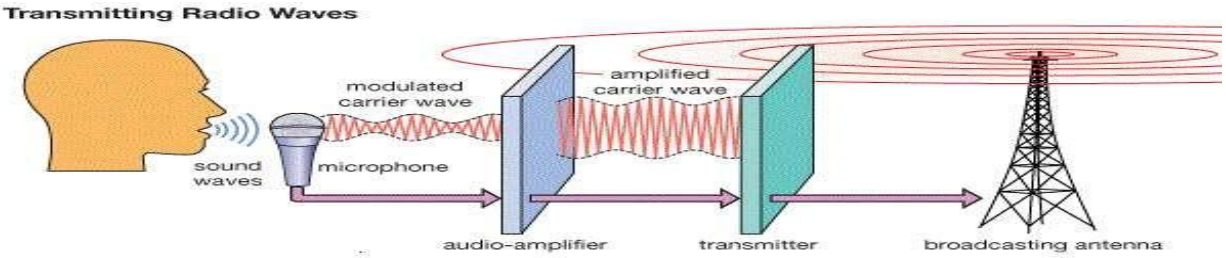
3.6.3 Unguided transmission media

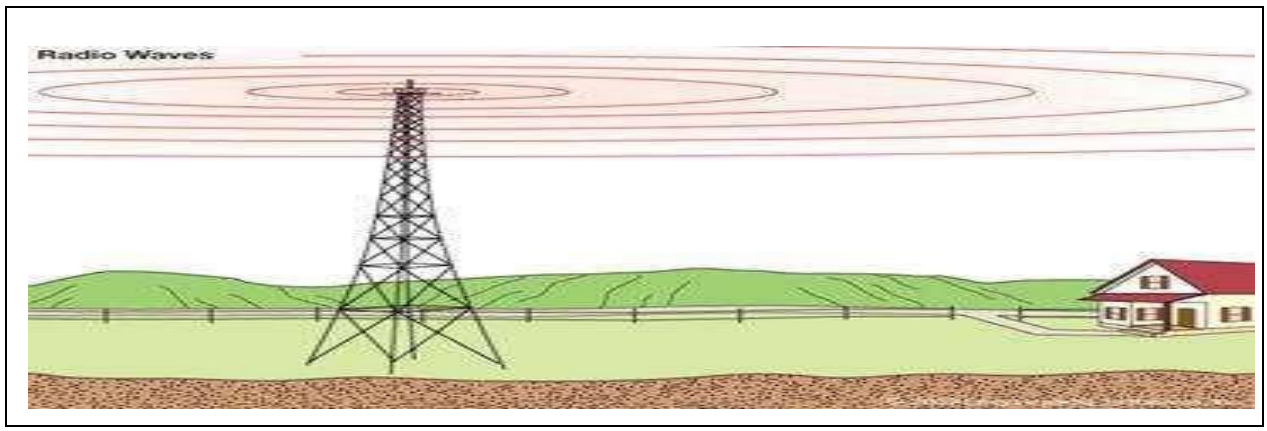
Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. The mediums used in wireless communications are air, vacuum and even water. Air is the most commonly used medium.

a. Wireless Transmission

Wireless transmission can be categorized into three broad groups namely radio waves,microwaves, infrared

1. Radio waves





Picture 3. 23: Radio Waves

Radio waves are normally **omnidirectional.** When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. Our FM radio stations, cordless phones and televisions are examples of multicasting.

2. Infrared

Picture 3. 24: Infrared devices

Infrared is used in devices such as the mouse, wireless keyboard and printers. Some manufacturers provide a special port called the IrDA port that allows a wireless keyboard to communicate with a PC.

Infrared signals have frequencies between 300 GHz to 400 THz. They are used for short-range communication. Infrared signals have high frequencies and cannot penetrate walls. Due to its short-range communication system, the use of an infrared communication system in one room will not be affected by the use of another system in the next room. This is why using an infrared TV remote control in our home will not interfere with the use of our neighbor's infrared TV remote control.

The disadvantages of using infrared

- Infrared signals cannot be used for long distance communication.
- Infrared waves can not be used outside of a building because sun's rays contain infrared waves that can interfere with communication.

3. Bluetooth

Bluetooth technology is designed to serve as a new way of connecting devices. Bluetooth technology has an advantage of being low investment and low energy consumption demanding. Th difference between Bluetooth and infrared is that Bluetooth allows communication when there is a barrier or a wall.

Pictur3.25:Bluetooth network

Wi-Fi (Wireless Fidelity)

Wi-Fi (Wireless Fidelity) is a standard that certifies that wireless devices in Wireless LAN to work together. It supports IEEE802.11b Ethernet standard.

Picture 3. 26: Wifi network

WI - FI uses radio signals to transmit high speed data over the wireless network, the Access Point is used to connect devices and it acts as the central device for Wireless LAN. Wireless devices can be: smartphones, PDAs, IPad, laptop and notebook.

APPLICATION ACTIVITY 3.12

General steps to connect to a WI-FI network near you

The following steps run through the general steps that anyone needs to take to get connected to the internet via WI-FI.

Step 1: Locate yourself in a property or public space that has a wireless router.

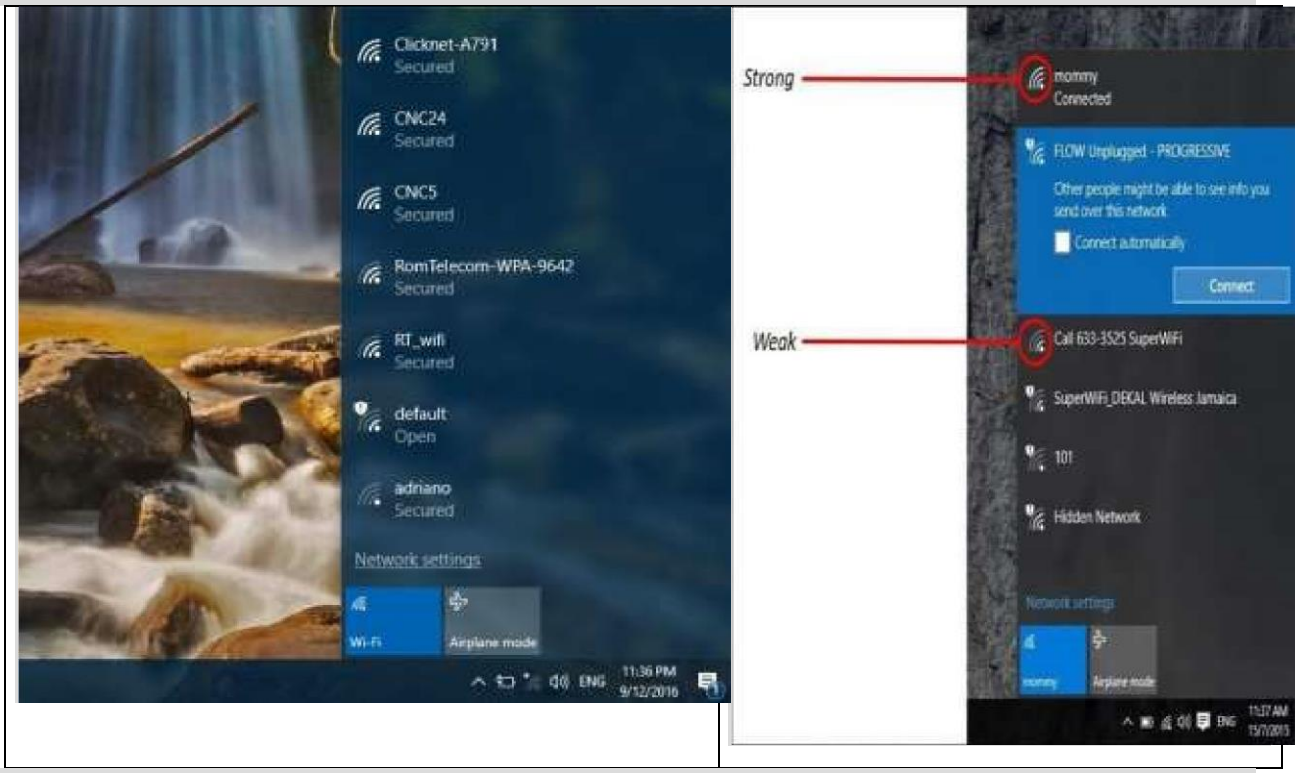
Step 2: Make sure that the device you're going to use is:

- Capable of connecting to the internet and
- Capable of connecting to WI-FI.

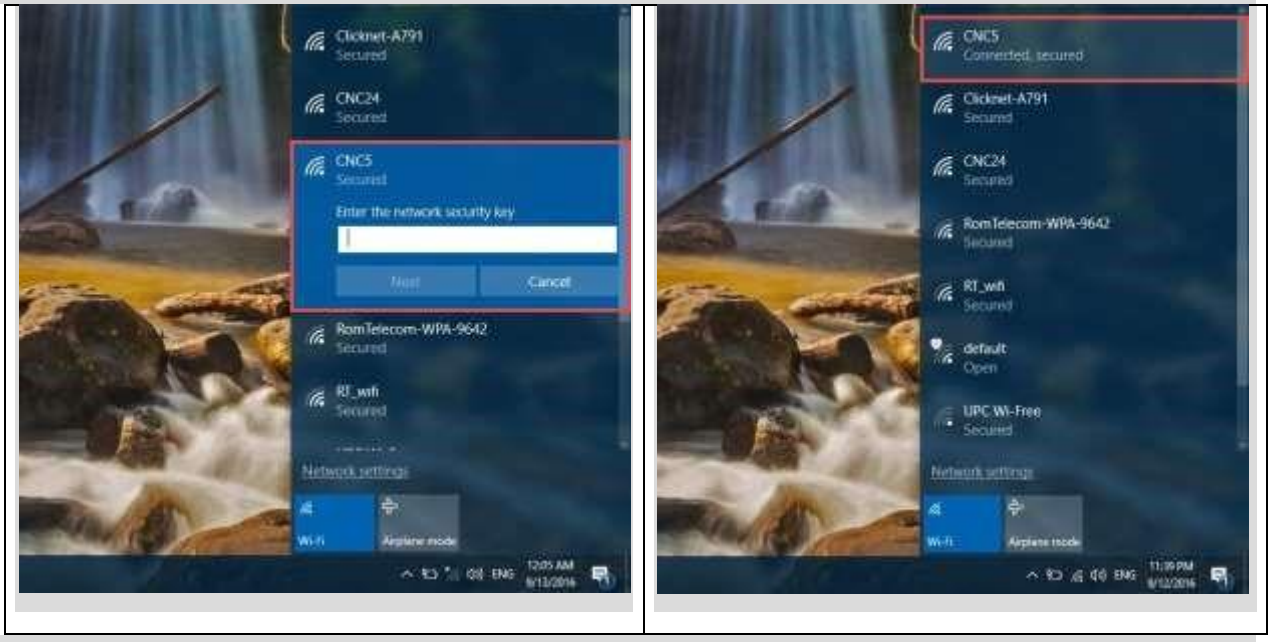
Step 3: Find out the name of the WI-FI network that the router in your location is transmitting.

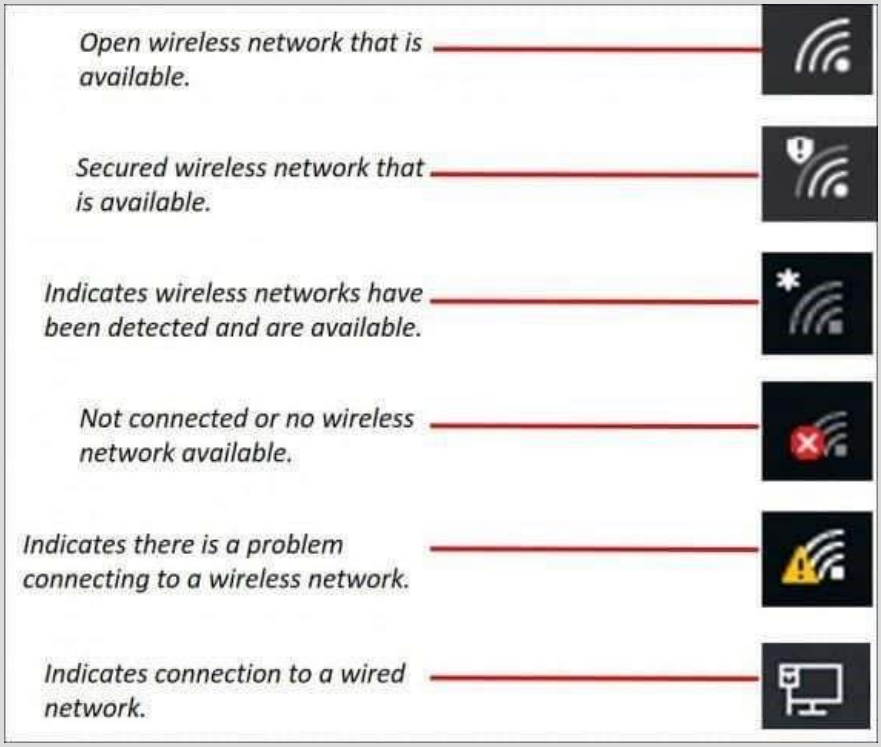
Step 4: Once you know the name of the WI -FI network, use your chosen device to find it.

Note: Following are steps to follow: navigate ***to Wi -Fi settings > turn Wi -Fi on > click on the name of your Wi -Fi network > click "connect" .***



Step 5: Many WI -FI networks are made private, with access restricted via a password. If your chosen WI -FI network is password protected, at this point it will ask you enter that password.





Cellular network generations

The G in 1G,2G, 3G and 4G stands for Generation, and they refer to 2nd, 3rd and 4th Generation of wireless technology. The newer generation is faster, more secure and more reliable. Briefly the difference between generations is expressed in terms of speed

Features found in each cellular network generation

1stGeneration:

•Offered in analog technology

•Enabled one user per channel(half duplex) **2nd Generation**:

- Digital cellular telephony
- Mobile 2G digital technologies increased voice capacity Delivering mobile voice services to the masses – more people, in more places
- Enabled more users per channel **3rd Generation:**
- High-speed digital cellular telephony (including video telephony)
- Mobile 3G evolved mobile for data introducing high-speed internet access for the first time
- Data enabling mobile broadband

4th Generation:

- 4G delivers up to 100Mbps for mobile access, and up to 1Gbps for wireless access.
- Most wireless carriers offering HSPA (High Speed Packet Access).
- IP-based "anytime, anywhere" voice, data, and multimedia telephony at faster data rates than 3G
- Evolving to provide more data capacity Delivering faster and better mobile broadband experience
- Download, browse, stream, and game faster than ever with faster and better connectivity **4G LTE** – LTE (Long Term Evolution) is one of the two standards offered within 4G, the 4G LTE is a type of 4G technology, and it delivers the best performance and speeds available today.

b. Location tracking through GPS

1. What is GPS?

GPS (Global Positioning System) is the U.S. satellite-based navigation system that uses a network of 24 satellites to provide 3-D locating data to GPS receivers on Earth.

In the 1980s, the U.S. Government made the decision to allow the system to be used by civilians and has since lifted restrictions previously placed on civilian GPS accuracy. Today, GPS is available for anyone to use.

2. How Does GPS Work?

All 24 GPS satellites circle the planet twice a day in a very specific orbit. During their travels, the satellite sends signal information to Earth. A GPS receiver receives the information from all available satellites and calculates the GPS receiver's exact location by comparing the time that a signal was transmitted by the satellite to the time the receiver receives the signal.

This provides the distance that the satellite is from the receiver. By using this difference from several satellites, the GPS receiver is able to determine the receiver's position with a high degree of accuracy and display on a map or chart. In order to provide an accurate 2D position consisting of latitude and longitude (and to track movement), GPS receivers require at least three GPS satellites signals to be received. If there are four or more

satellites in view, then the 3D position of the GPS receiving unit (latitude, longitude, and altitude) can be determined.

Access methods

CSMA/CD

CSMA/CA

Token passing

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a modification of CSMA in which each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes two computers attempt to transmit at the same instant. When this happens, a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. This removes the possibility for collisions to occur.

Token passing

On a local area network, token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate. In contrast to polling access methods, there is no pre-defined "master" node. Wikipedia

I I.3 IP addresses

An **IP address** is a logical address for a network adapter. The IP address uniquely identifies computers on a TCP/IP network.

An IP address can be private - for use on a local area network (LAN) - or public - for use on the Internet or other wide area network (WAN).

Internet Protocol (IP) technology was developed in the 1970s to support some of the first research computer networks. Today, IP has become a worldwide standard for home and business networking as well. Our network routers, Web browsers, email programs, instant messaging software - all rely on IP or other network protocols layered on top of IP.

Two versions of IP technology exist today. Essentially all home computer networks use IP version 4 (IPv4), but an increasing number of educational and research institutions have adopted the next generation IP version 6 (IPv6).

IPv4 Addressing Notation

An IPv4 address consists of four bytes (32 bits). These bytes are also known as octets. Octets can take any value between 0 and 255.

For readability purposes, humans typically work with IP addresses in a notation called **dotted decimal**. This notation places periods between each of the four numbers (octets) that comprise an IP address. For example, an IP address that computers see as

00001010 00000000 00000000 00000001

is written in dotted decimal as10.0.0.1Because each byte contains 8 bits, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255. Therefore, the full range of IP addresses is from**0.0.0.0** through **255.255.255.255**. That represents a total of 4,294,967,296 possible IP addresses.

IPv6 Addressing Notation

IP addresses change significantly with IPv6. IPv6 addresses are 16 bytes (128 bits) long rather than four bytes (32 bits). This larger size means that IPv6 supports more than

300,000,000,000,000,000,000,000,000,000,000,000,000possible addresses! In the coming years, as an increasing number of cell phones, PDAs, and other consumer electronics expand their networking capability, the smaller IPv4 address space will likely run out and IPv6 address become necessary.IPv6 addresses are generally written in the following form:

hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh

In this **full notation**, pairs of IPv6 bytes are separated by a colon and each byte in turns is represented as a pair of hexadecimal numbers, like in the following example:

E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420

As shown above, IPv6 addresses commonly contain many bytes with a zero value.**Shorthand notation** in IPv6 removes these values from the text representation (though the bytes are still present in the actual network address) as follows:

E3D7::51F4:9BC8:C0A8:6420

Finally, many IPv6 addresses are extensions of IPv4 addresses. In these cases, the rightmost four bytes of an IPv6 address (the rightmost two byte pairs) may be rewritten in the IPv4 notation. Converting the above example to **mixed notation** yields

E3D7::51F4:9BC8:192.168.100.32

IPv6 addresses may be written in any of the full, shorthand or mixed notation illustrated above.

Common IP (IPv4) Addresses

10.0.0.1

10.0.0.1 is sometimes called a default gateway address as it typically represents the local side of a router's connection to the Internet. 10.0.0.1 is more commonly found in business networks than in homes, which tend to use routers having default addresses in the 192.168.x.x series. Both the 10.x.x.x and 192.168.x.x series are private IP address ranges.

127.0.0.1

The IP address **127.0.0.1** is a special purpose address reserved for use on each computer. 127.0.0.1 is conventionally a computer's loopback address.

Loopback is a test mechanism of network adapters.

Messages sent to 127.0.0.1 do not get delivered to the network. Instead, the adapter intercepts all loopback messages and returns them to the sending application. IP applications often use this feature to test the behavior of their network interface.

Network software and utilities can use 127.0.0.1 to access a local computer's TCP/IP network resources. Messages sent to loopback IP addresses like 127.0.0.1 do not reach outside to the local area network (LAN) but instead are automatically re-routed by the computer's own network adapter back to the receiving end of the TCP/IP stack.

Typically all IP addresses in the range 127.0.0.1 - 127.255.255.255 are reserved for private use, but 127.0.0.1 is by convention the loopback address in almost all cases.

192.160.0.1

The IP address **192.168.0.1** is the default for certain home broadband routers, principally various D-Link and Netgear models. This address is set by the manufacturer at the factory, but you can change it at any time using the network router's administrative console.

192.168.0.1 is a private IPv4 network address. Home routers can use it to establish the default gateway. On such routers, you can access its administrative console by pointing a Web browser to http://192.168.0.1.

Any brand of router, or any computer on a local network for that matter, can be set to use this address or a comparable private IPv4 address. As with any IP address, only one device on the network should use 192.168.0.1 to avoid address conflicts.

192.168.1.1

192.168.1.1 is an IP address normally used by Linksys broadband routers. Some other brands of network routers also use this same address. While technically a computer, printer or other device can be set up to use this address instead of a router, that's uncommon.

192.168.2.1

192.168.2.1 is the default IP address for certain models of home broadband routers. 192.168.2.1 is a private IPv4 network address meaning that you cannot connect to a router from outside the home network using this address. Instead, you must use the router's public IP address.

I I.4 Mask

Subnet masks are 32 bit values that allow the recipient of IP packets to distinguish the network ID portion of the IP address from the host ID.

NETID:

-Network portion of an IP Address.
-A network ID refers to a part of a TCP/IP address that is used to identify the subnet that a host may be on.

HOST ID:

The portion of the IP address that identifies a particular computer within a particular network ID.

The subnet masks are created by assigning 1's to network ID bits and 0's to host ID bits. The 32 bits is then converted to dotted- decimal notations.

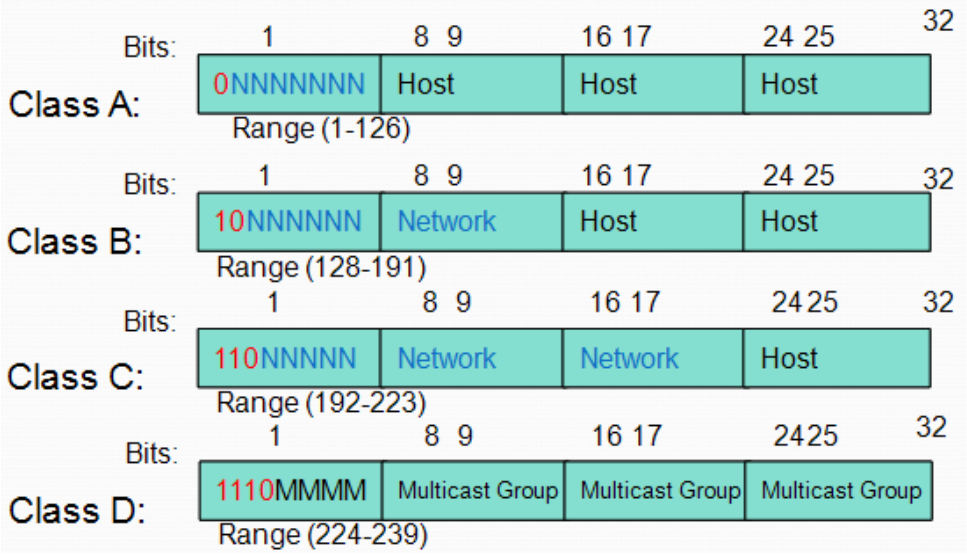
Address class	Bits for subnet masks	Subnet mask
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

I.5 IP address Classes

IP address classes include:

1. Class A 2. Class B 3. Class C 4.Class D : multicast 5.Class E : reserved

Illustration of IP classes and their ranges



Class A

This class is assigned to very large Networks, such as major international companies.

Class A licenses assigns numbers to be used in the first octet (leftmost) of the address, which becomes the network address.

The other three octets on the right of the IP can be used for host addresses that identify each host on this network.

Example:

If a company assigns 87 as its class A network address, then 87 is issued as the first octet for every host on that network.

Example of IP addresses for hosts on this network are 87.0.0.1, 87.0.0.2, 87.0.0.3 etc.

NET HOST OR NODE

87 .0.0.2

The last octet does not use 0 or 255 as a value. Example, 87.0.0.0 or 87.0.0.255 are not valid on class A.

The number of hosts in class A are approximately 16,000

i.e.

87.255 * 255 * 254 = 16,516.350

Class B

Class B is used for the medium sized networks.

The class B license assigns a number for each of the first two left most octets, leaning the last two octets for host addresses.

The possible number of hosts in class B are about 65,000.

I.e. 255 * 255 = 65,536

The first octet for class B license is between 128 and 191, which gives about 63 different values for a class B first octet.

The second number can be between 0 and 255.

There are approximately 16,000 networks in class B.

Ie 63 * 255 = 16,128

Example:

Suppose a company assigned an IP address 135.18 as the network address for its class B license. The first octets for all the networks will be 135.18 and the last two octets are used for host addresses.

Example: NET HOST OR NODE

135.18 .0.1

Class c addresses are commonly used for small to mid- size networks.

A class C license assigns three octets as the network addresses and can have 254 host addresses.

The three first octets are assigned to the Network ID

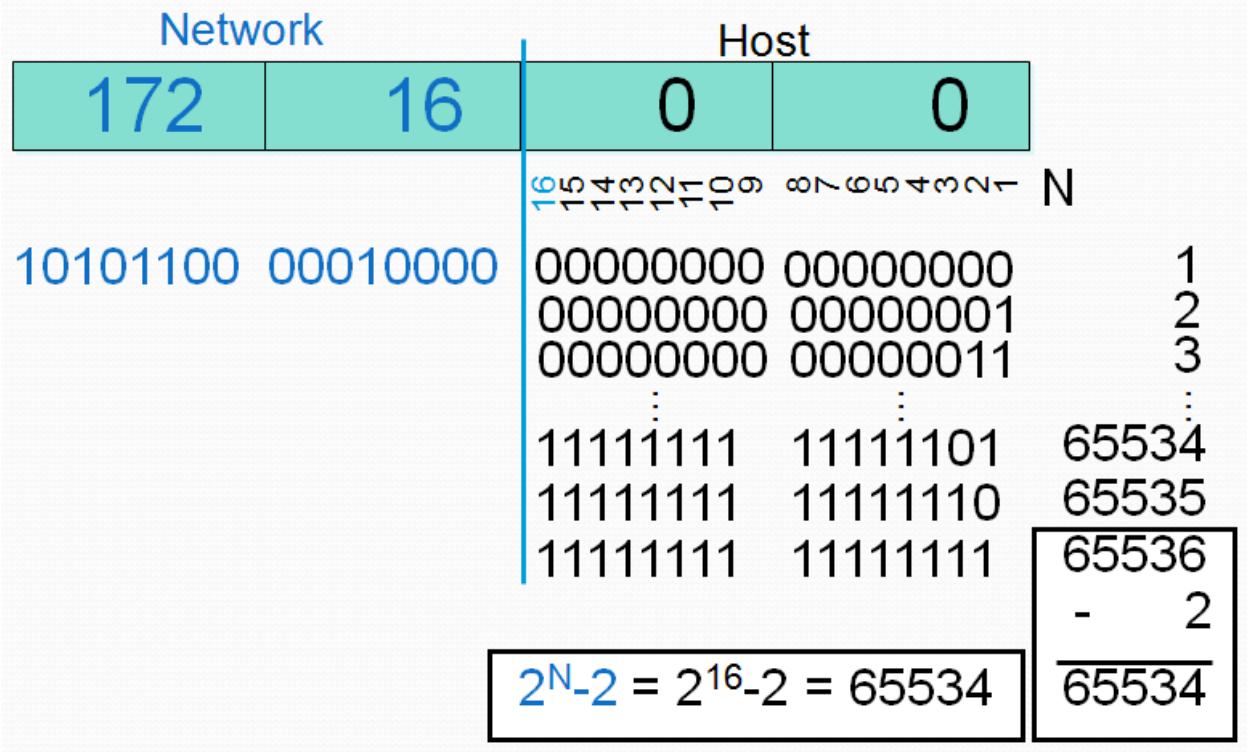
The first number of the class C is between 192 and 254.

Example:

A company can be assigned a class C license for its network with a network address of 200.80.15. Some of the IP addresses in such a network are

200.80.15.1, 200.80.15.0,200.80.15.0 etc.

Determining Available Host Adresses



IP Address Classes Exercise

Find IP classes, network and host for the following addresses:

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

Private IP Addresses

- The people who created the IP addressing scheme also created what we call private IP addresses.
- These addresses can be used on a private network, but they're not routable through the Internet.
- This is conveniently saves valuable IP address space.
- To connect private network on public network/global network we need to use something called a *Network Address Translation (NAT), which basically* takes a private IP address and converts it for use on the Internet.

Private IP Addresses

Several networks are reserved for private use and cannot be used on the Internet. They include:

A few IP addresses are reserved for special use by TCP/IP and should not be used.

They include:

255.255.255.255	Used to Broadcast Messages
0.0.0.0	Unassigned IP address
127.0.0.1	Acts as a loop back address.

It's used by the host computer to send messages back to itself. It's used for troubleshooting and network testing

Definitions

1. *Loopback address:* An address that sends outgoing signals back to the same computer for testing.

2. Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems (included in Windows 98, ME, 2000, XP etc) that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. APIPA serves as a DHCP server failover mechanism and makes it easier to configure and support small local area networks (LANs).

If no DHCP server is currently available (either because the server is temporarily down or because none exists on the network), the computer selects an IP address from a range of addresses (from 169.254.0.0 - 169.254.255.255) reserved by the Internet Assigned Numbers Authority (IANA) for that purpose. The client uses Address Resolution Protocol (ARP) to ensure that the chosen address is not already being used by another network computer. Once the computer has assigned itself an

IP address, it can communicate over TCP/IP with other computers on the LAN that are either configured for APIPA or are manually set to the correct address range and a subnet mask value of 255.255.0.0. APIPA is enabled by default, but can be disabled in some cases. DHCP messages notify the user when they are switched between DHCP addressing and APIPA

3. Multicast: multicast is a mechanism for defining groups of nodes and sending IP messages to that group rather than to every node on the LAN (broadcast) or just one other node (**unicast**).

Multicast is mainly used on research networks. As with Class E, Class D addresses should not be used by ordinary nodes on the Internet.

4.Broadcast address: A **broadcast address** is a logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. A message sent to a broadcast address is typically received by all network-attached hosts, rather than by a specific host.

Summary

Layer 2 broadcasts These are sent to all nodes on a LAN.
Broadcasts (layer 3) These are sent to all nodes on the network.
Unicast These are sent to a single destination host.
Multicast These are packets sent from a single source and transmitted to many devices on different networks.

Reserved IP

A 10.x.x.x

B 172.16.x.x through 172.31.x.x

C 192.168.x.x

169.254.x.x Microsoft reserved

127.x.x.x for loopback

I I.6 Sub network
Prior to 1981, IP addresses used only the first 8 bits to specify the network portion of the address. In 1981, RFC 791 (Request For Comments for Internet Protocol) modified the IPv4 32-bit address to allow for three different classes:

- Class A addresses used 8 bits for the network portion of the address,
- Class B used 16 bits,
- Class C used 24 bits.

This format became known as classful IP addressing. By using them, IP address space was depleting rapidly. The Internet Engineering Task Force (IETF) introduced Classless Inter-Domain Routing (CIDR) which uses Variable Length Subnet Masking (VLSM) to help conserve address space. VLSM is simply subnetting a subnet.

With the introduction of CIDR and VLSM, ISPs could now assign one part of a classful network to one customer and different part to another customer.

Reminder on IP Class Ranges

The designers of the IP address scheme said that the first bit of the first byte in a Class A network address must always be off, or 0. This means a Class A address must be between 0 and 127 in the first byte, inclusive.
Consider the following network address:
0xxxxxxx
If we turn the other 7 bits all off and then turn them all on, we'll find the Class A range of network addresses:
00000000 = 0
01111111 = 127
So, a Class A network is defined in the first octet between 0 and 127, and it can't be less or more. 0 or 127 are reserved.
In a Class B network, the RFCs state that the first bit of the first byte must always be turned on but the second bit must always be turned off. If you turn the other 6 bits all off and then all on, you will find the range for a Class B network:
10000000 = 128
10111111 = 191
As you can see, a Class B network is defined when the first byte is configured from 128 to 191.

For Class C networks, the RFCs define the first 2 bits of the first octet as always turned on, but the third bit can never be on. Following the same process as the previous classes, convert from binary to decimal to find the range. Here's the range for a Class C network:
11000000 = 192
11011111 = 223
So, if you see an IP address that starts at 192 and goes to 223, you'll know it is a Class C IP address.

Definition

1. Sub netting consists of dividing a large network into smaller networks. For instance if you had a network with 100 computers you could divide this into 5 subnets with 20 computers on it.

2.Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you are only able to use one network from your Class A, B, or C network, which is unrealistic.

II.6.1 How to create subnets?

To create subnetworks, you take bits from the host portion of the IP address and reserve them to define the subnet address. This means fewer bits for hosts, so the more subnets.

In subnetting there is a slash notation (/) means how many bits are turned on (1s). Obviously, the maximum could only be /32 because a byte is 8 bits and there are 4 bytes in an IP address: (4 * 8 = 32). The largest subnet mask available (regardless of the class of address) can only be a /30 because you've got to keep at least 2 bits for host bits.

Listing of every available subnet mask and its equivalent CIDR slash notation

Subnet Mask	CIDR Value	Subnet Mask	CIDR Value	Subnet Mask	CIDR Value	Subnet Mask	CIDR Value	Subnet Mask	CIDR Value
255.0.0.0	/8	255.248.0.0	/13	255.355.192.0	/18	255.255.254.0	/23	255.255.255.240	/28
255.128.0.0	/9	255.252.0.0	/14	255.255.224	/19	255.255.255.0	/24	255.255.255.248	/29
255.192.0.0	/10	255.254.0.0	/15	255.255.240.0	/20	255.255.255.128	/25	255.255.255.252	/30
255.224.0.0	/11	255.255.0.0	/16	255.255.248.0	/21	255.255.255.192	/26		
255.240.0.0	/12	255.255.128.0	/17	255.255.252.0	/22	255.255.255.224	/27		

The /8 through /15 can only be used with Class A network addresses. /16 through /23 can be used by Class A and B network addresses. /24 through /30 can be used by Class A, B, and C network addresses.

Subnetting a Class C Address

In a Class C address, only 8 bits are available for defining the hosts. Note that subnet bits start at the left and go to the right, without skipping bits. This means that the only Class C subnet masks can be the following:

Binary	Decimal	CIDR
00000000	0	/24
10000000	128	/25
11000000	192	/26
11100000	224	/27
11110000	240	/28
11111000	248	/29
11111100	252	/30

We can't use a /31 or /32 because we have to have at least 2 host bits for assigning IP addresses to hosts.

When you've chosen a possible subnet mask for your network and need to determine the number of subnets, valid hosts, and broadcast addresses of a subnet that the mask provides, all you need to do is answer five simple questions:

1. How many subnets does the chosen subnet mask produce?
2. How many valid hosts per subnet are available?
3. What are the valid subnets?
4. What's the broadcast address of each subnet?
5. What are the valid hosts in each subnet?

Guideline on providing answers to those questions:

How many subnets?

2^x = number of subnets. *x* is the number of masked bits, or the 1s.
For example, in 11000000, the number of 1s gives us 2^2 subnets. In this example, there are 4 subnets.

How many hosts per subnet?

$2^y - 2$ = number of hosts per subnet. *y* is the number of unmasked bits, or the 0s. For example, in 11000000, the number of 0s gives us $2^6 - 2$ hosts.
In this example, there are 62 hosts per subnet. You need to subtract 2 for the subnet address and the broadcast address, which are not valid hosts.

What are the valid subnets?

256 – subnet mask = block size, or increment number. An example would be 256 – 192 = 64. The block size of a 192 mask is always 64.
Start counting at zero in blocks of 64 until you reach the subnet mask value and these are your subnets. 0, 64, 128, 192.
What's the broadcast address for each subnet?

Since we counted our subnets as 0, 64, 128, and 192, the broadcast address is always the number right before the next subnet.

For example, the 0 subnet has a broadcast address of 63 because the next subnet is 64.

The 64 subnet has a broadcast address of 127 because the next subnet is 128. And so on. And remember, the broadcast address of the last subnet is always 255.

What are the valid hosts?
Valid hosts are the numbers between the subnets, omitting the all 0s and all 1s.

For example, if 64 is the subnet number and 127 is the broadcast address, then 65–126 is the valid host range—it's *always* the numbers between the subnet address and the broadcast address.

Subnetting Practice Example (Class C Addresses)

Practice Example 1: 255.255.255.128 (/25)

Since 128 is 10000000 in binary, there is only 1 bit for subnetting and 7 bits for hosts. Let us subnet the Class C network address 192.168.10.0.
192.168.10.0 = Network address
255.255.255.128 = Subnet mask
Now, let's answer the five questions:

1. **How many subnets?**

Since 128 is 1 bit on (**1**0000000), the answer would be 2^1 =2 subnets

2. **How many hosts per subnet?**

We have 7 host bits off (1**0000000**), so the equation would be $2^7 - 2 = 126$ hosts.

3. **What are the valid subnets?**

256 – 128 = 128. Remember, we'll start at zero and count in our block size, so our subnets are 0, 128.

4. **What's the broadcast address for each subnet?**

The number right before the value of the next subnet is all host bits turned on and equals the broadcast address. For the zero subnet, the next subnet is 128, so the broadcast of the 0 subnet is 127.

2. **What are the valid hosts?**

These are the numbers between the subnet and broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address. This way, the valid hosts are obvious. The following table shows the 0 and 128 subnets, the valid host ranges of each, and the broadcast address of both subnets:

Subnet	0	128
First host	1	129
Last host	126	254
Broadcast	127	255

NO	SUBNETS	START IP	LAST IP	BROADCAST ADDRESS
1	192.168.10.0	192.168.10.1	192.168.10.126	192.168.10.127
2	192.168.10.128	192.168.10.129	192.168.10.254	192.168.10.255

Broadcast address : A broadcast address is a special type of networking address that is reserved for sending messages to all nodes (i.e., devices attached to the network) on a givennetwork or network segment.

Practice Example 2:

255.255.255.192 (/26)
Subnet the network address 192.168.10.0 using the subnet mask 255.255.255.192.

192.168.10.0 = Network address
255.255.255.192 = Subnet mask

Now, let's answer the big five:

How many subnets?
Since 192 is 2 bits on (**11**000000), the answer would be 2^2=4 subnets

How many hosts per subnet?
We have 6 host bits off (11**000000**), so the equation would be $2^6 - 2 = 62$ hosts.

What are the valid subnets?
256 – 192 = 64. Remember, we start at zero and count in our block size, so our subnets are:

0, 64, 128, and 192.

What's the broadcast address for each subnet?

The number right before the value of the next subnet is all host bits turned on and equals the broadcast address. For the zero subnet, the next subnet is 64, so the broadcast address for the zero subnet is 63.

What are the valid hosts?

These are the numbers between the subnet and broadcast address. The easiest way to find the hosts is to write out the subnet address and the broadcast address.

This way, the valid hosts are obvious.
The following table shows the 0, 64, 128, and 192 subnets, the valid host ranges of each, and the broadcast address of each subnet:

NO	SUBNETS	START IP	LAST IP	BROADCAST ADDRESS
1	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
3	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
4	192.168.10.192	192.168.10.192	192.168.10.254	192.168.10.255

Practice Example 3:

255.255.255.224 (/27)

This time, we'll subnet the network address 192.168.10.0 and subnet mask 255.255.255.224.

192.168.10.0 = Network address
255.255.255.224 = Subnet mask

1.How many subnets?

224 is 11100000, so our equation would be 2^3 = 8 subnets

2. How many hosts?
$2^5 - 2 = 30$.

3. What are the valid subnets?

256 – 224 = 32. We just start at zero and count to the subnet mask value in blocks (increments) of 32:

0, 32, 64, 96, 128, 160, 192, and 224.

4. What's the broadcast address for each subnet (always the number right before the next subnet)?
31, 63, 95, 127, 159, 191, 223,225
5. What are the valid hosts (the numbers between the subnet number and the broadcast address)?

The following table gives you all the subnets for the 255.255.255.224 Class C subnet mask:
The subnet address 0 32 64 96 128 160 192 224
The first valid host 1 33 65 97 129 161 193 225
The last valid host 30 62 94 126 158 190 222 254
The broadcast address 31 63 95 127 159 191 223 255

Table which summarize:

NO	SUBNETS	START IP	LAST IP	BROADCAST ADDRESS
1	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.31
2	192.168.10.32	192.168.10.65	192.168.10.126	192.168.10.63
3	192.168.10.64	192.168.10.129	192.168.10.190	192.168.10.95
4	192.168.10.96	192.168.10.192	192.168.10.254	192.168.10.127
5	192.168.10.128	192.168.10.129	192.168.10.158	192.168.10.159
6	192.168.10.160	192.168.10.161	192.168.10.190	192.168.10.191
7	192.168.10.192	192.168.10.193	192.168.10.222	192.168.10.223
8	192.168.10.224	192.168.10.225	192.168.10.254	192.168.10.255

Practice Example 4:

255.255.255.240 (/28)

Let's practice on another one:
192.168.10.0 = Network address
255.255.255.240 = Subnet mask

Subnets? 240 is 11110000 in binary. $2^4 = 16$
Hosts? 4 host bits, or $2^4 - 2 = 14$.
Valid subnets? 256 – 240 = 16.
Start at 0:

0 + 16 = 16.
16 + 16 = 32.
32 + 16 = 48.
48 + 16 = 64.
64 + 16 = 80.
80 + 16 = 96.
96 + 16 = 112.
112 + 16 = 128.
128 + 16 = 144.
144 +16 = 160.
160 + 16 = 176.
176 + 16 = 192.
192 + 16 = 208.
208 + 16 = 224.
224 + 16 = 240.

Broadcast address for each subnet?

Valid hosts?

To answer the last two questions, check out the following table.

The following table shows the available subnets, hosts, and broadcast addresses provided from a Class C 255.255.255.240 mask:
Subnet 0 16 32 48 64 80 96 112 128 144 160 176 192 208 224 240
First host 1 17 33 49 65 81 97 113 129 145 161 177 193 209 225 241
Last host 14 30 46 62 78 94 110 126 142 158 174 190 206 222 238 254
Broadcast 15 31 47 63 79 95 111 127 143 159 175 191 207 223 239 255

Table of subnets start IP, Last IP, Broadcast Address

NO	SUBNETS	START IP	LAST IP	BROADCAST ADDRESS
1	192.168.10.0	192.168.10.1	192.168.10.	192.168.10.15
2	192.168.10.16	192.168.10.17	192.168.10.	192.168.10.31
3	192.168.10.32	192.168.10.33	192.168.10.	192.168.10.47
4	192.168.10.48	192.168.10.49	192.168.10.	192.168.10.63
5	192.168.10.64	192.168.10.65	192.168.10.	192.168.10.79
6	192.168.10.80	192.168.10.81	192.168.10.	192.168.10.95
7	192.168.10.96	192.168.10.97	192.168.10.	192.168.10.111
8	192.168.10.112	192.168.10.113	192.168.10.	192.168.10.127
9	192.168.10.128	192.168.10.129	192.168.10.	192.168.10.143
10	192.168.10.144	192.168.10.145	192.168.10.	192.168.10.159
11	192.168.10.160	192.168.10.161	192.168.10.	192.168.10.175
12	192.168.10.176	192.168.10.177	192.168.10.	192.168.10.191

13	192.168.10.192	192.168.10.193	192.168.10.	192.168.10.207
14	192.168.10.208	192.168.10.209	192.168.10.	192.168.10.223
15	192.168.10.224	192.168.10.225	192.168.10.	192.168.10.239
16	192.168.10.240	192.168.10.241	192.168.10.	192.168.10.255

Practice Example 5:

255.255.255.248 (/29)
Let's keep practicing:
192.168.10.0 = Network address
255.255.255.248 = Subnet mask

Subnets? 248 in binary = 11111000. $2^5 = 32$.

Hosts? $2^3 - 2 = 6$.
Valid subnets? 256 – 248 = 8
0, 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120,
128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, and 248.
Broadcast address for each subnet?
Valid hosts?
Take a look at the following table. It shows some of the subnets (first four and last four only), valid hosts, and broadcast addresses for the Class C 255.255.255.248 mask:
Subnet 0 8 16 24 … 224 232 240 248
First host 1 9 17 25 … 225 233 241 249
Last host 6 14 22 30 … 230 238 246 254
Broadcast 7 15 23 31 … 231 239 247 255

Practice Example 6:

255.255.255.252 (/30)
Just one more:
192.168.10.0 = Network address
255.255.255.252 = Subnet mask
Subnets? 64.
Hosts? 2.
Valid subnets? 0, 4, 8, 12, etc., all the way to 252.
Broadcast address for each subnet (always the number right before the next subnet)?
Valid hosts (the numbers between the subnet number and the broadcast address)?
The following table shows you the subnet, valid host, and broadcast address of the first four and last four subnets in the 255.255.255.252 Class C subnet:
Subnet 0 4 8 12 … 240 244 248 252
First host 1 5 9 13 … 241 245 249 253
Last host 2 6 10 14 … 242 246 250 254
Broadcast 3 7 11 15 … 243 247 251 255

When you see a subnet mask or slash notation (CIDR), you should know the following:

/25 What do we know about a /25?

128 mask
1 bits on and 7 bits off (10000000)
Block size of 128
2 subnets, each with 126 hosts

/26 What do we know about a /26?

192 mask
2 bits on and 6 bits off (11000000)
Block size of 64
4 subnets, each with 62 hosts

/27 What do we know about a /27?

224 mask
3 bits on and 5 bits off (11100000)
Block size of 32
8 subnets, each with 30 hosts

/28 What do we know about a /28?

240 mask
4 bits on and 4 bits off
Block size of 16
16 subnets, each with 14 hosts

/29 What do we know about a /29?

248 mask
5 bits on and 3 bits off
Block size of 8
32 subnets, each with 6 hosts

/30 What do we know about a /30?

252 mask
6 bits on and 2 bits off
Block size of 4
64 subnets, each with 2 hosts

Subnetting a Class A IP Address

Before we start, let's look at all the possible Class B subnet masks first. Notice that we have a lot more possible subnet masks than we do with a Class C network address:

255.255.0.0	(/16)		
255.255.128.0	(/17)	255.255.255.0	(/24)
255.255.192.0	(/18)	255.255.255.128	(/25)
255.255.224.0	(/19)	255.255.255.192	(/26)
255.255.240.0	(/20)	255.255.255.224	(/27)
255.255.248.0	(/21)	255.255.255.240	(/28)
255.255.252.0	(/22)	255.255.255.248	(/29)
255.255.254.0	(/23)	255.255.255.252	(/30)

We know the Class B network address has 16 bits available for host addressing. This means we can use up to 14 bits for subnetting (because we have to leave at least 2 bits for host addressing). Using a /16 means you are not subnetting with class B, but it is a mask you can use.

The process of subnetting a Class B network is pretty much the same as it is for a Class C, except that you just have more host bits and you start in the third octet. Use the same subnet numbers for the third octet with Class B that you used for the fourth octet with Class C, but add a zero to the network portion and a 255 to the broadcast section in the fourth octet. The following table shows you an example host range of two subnets used in a Class B 240 (/20) subnet mask:

First subnet	16.0	32.0
Second subnet	31.255	47.255

Subnetting Practice Examples: Class B Addresses

Subnetting Class B addresses is the same as subnetting with Class C, except we start in the third octet—with the exact same numbers!

Practice Example 1B:
255.255.128.0 (/17)
172.16.0.0 = Network address
255.255.128.0 = Subnet mask
1.Subnets? 2^1 =2 (same as Class C).
2.Hosts? 2^{15} -2= 32,766 (7 bits in the third octet, and 8 in the fourth).
3.Valid subnets? 256 – 128 = 128. 0, 128. Remember that subnetting is performed in the third octet, so the subnet numbers are really 0.0 and 128.0, as shown in the next table. These are the exact numbers we used with Class C; we use them in the third octet and add a 0 in the fourth octet for the network address.
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the two subnets available, the valid host range, and the broadcast address of each:

Subnet	0.0	128.0
First host	0.1	128.1
Last host	127.254	255.254
Broadcast	127.255	255.255

Notice that we just added the fourth octet's lowest and highest values and came up with the answers. And again, it's done exactly the same way as for a Class C subnet. We just use the same numbers in the third octet and added 0 and 255 in the fourth octet.

Practice Example 2B: 255.255.192.0 (/18)

172.16.0.0 = Network address
255.255.192.0 = Subnet mask
1.Subnets? 2^2=4
2.Hosts? 2^{14}-2=16,382 (6 bits in the third octet, and 8 in the fourth).
3.Valid subnets? 256 – 192 = 64. 0, 64, 128, 192. Remember that the subnetting is performed in the third octet, so the subnet numbers are really 0.0, 64.0, 128.0, and 192.0, as shown in the next table.
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the four subnets available, the valid host range, and the broadcast address of each:

Subnet	0.0	64.0	128.0	192.0
First host	0.1	64.1	128.1	192.1
Last host	63.254	127.254	191.254	255.254
Broadcast	63.255	127.255	191.255	255.255

Much the same as it is for a Class C subnet—we just added 0 and 255 in the fourth octet for each subnet in the third octet.

Practice Example 3B: 255.255.240.0 (/20)

172.16.0.0 = Network address
255.255.240.0 = Subnet mask
1.Subnets? 2^4=15
2.Hosts? 2^{12}-2=4094
3.Valid subnets? 256 – 240 = 0, 16, 32, 48, etc., up to 240. Notice that these are the same numbers as a Class C 240 mask – we just put them in the third octet and add a 0 and 255 in the fourth octet.
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the first four subnets, valid hosts, and broadcast addresses in a Class B 255.255.240.0 mask:

Subnet	0.0	16.0	32.0	48.0
First host	0.1	16.1	32.1	48.1
Last host	15.254	31.254	47.254	63.254
Broadcast	15.255	31.255	47.255	63.255

Practice Example 4B: 255.255.254.0 (/23)

172.16.0.0 = Network address
255.255.254.0 = Subnet mask
1.Subnets? 2^7=128
2.Hosts? 2^9-2=510
3.Valid subnets?
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the first five subnets, valid hosts, and broadcast addresses in a Class B 255.255.254.0 mask:

Subnet	0.0	2.0	4.0	6.0	8.0
First host	0.1	2.1	4.1	6.1	8.1
Last host	1.254	3.254	5.254	7.254	9.254
Broadcast	1.255	3.255	5.255	7.255	9.255

Practice Example 5B: 255.255.255.0 (/24)

Contrary to popular belief, 255.255.255.0 used with a Class B network address is not called a Class B network with a Class C subnet mask. It's amazing how many people see this mask used in a Class B network and think it's a Class C subnet mask. This is a Class B subnet mask with 8 bits of subnetting—it's considerably different from a Class C mask. Subnetting this address is fairly simple:

172.16.0.0 = Network address
255.255.255.0 = Subnet mask
1.Subnets? 28=256
2.Hosts? 28-2=254
3.Valid subnets? 256 – 255 = 1. 0, 1, 2, 3, etc., all the way to 255.
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the first four and last two subnets, the valid hosts, and the broadcast addresses in a Class B 255.255.255.0 mask:

Subnet	0.0	1.0	2.0	3.0	...	254.0	255.0
First host	0.1	1.1	2.1	3.1	...	254.1	255.1
Last host	0.254	1.254	2.254	3.254	...	254.254	255.254
Broadcast	0.255	1.255	2.255	3.255	...	254.255	255.255

Practice Example 6B: 255.255.255.128 (/25)

This is one of the hardest subnet masks you can play with. And worse, it actually is a really good subnet to use in production because it creates over 500 subnets with 126 hosts for each subnet—a nice mixture.

172.16.0.0 = Network address
255.255.255.128 = Subnet mask

1.Subnets? 29=512
2.Hosts? 27-2=126
3.Valid subnets? Okay, now for the tricky part. 256 – 255 = 1. 0, 1, 2, 3, etc. for the third octet. But you can't forget the one subnet bit used in the fourth octet. Remember how to figure one subnet bit with a Class C mask. You figure this the same way. You actually get two subnets for each third octet value, hence the 512 subnets.

For example, if the third octet is showing subnet 3, the two subnets would actually be 3.0 and 3.128.

4.Broadcast address for each subnet?
5.Valid hosts?

The following table shows how you can create subnets, valid hosts, and broadcast addresses using the Class B 255.255.255.128 subnet mask (the first eight subnets are shown, and then the last two subnets):

Subnet	0.0	0.128	1.0	1.128	2.0	2.128	3.0	3.128	...	255.0	255.128
First host	0.1	0.129	1.1	1.129	2.1	2.129	3.1	3.129	...	255.1	255.129
Last host	0.126	0.254	1.126	1.254	2.126	2.254	3.126	3.254	...	255.126	255.254
Broadcast	0.127	0.255	1.127	1.255	2.127	2.255	3.127	3.255	...	255.127	255.255

Practice Example 7B: 255.255.255.192 (/26)

Now, this is where Class B subnetting gets easy. Since the third octet has a 255 in the mask section, whatever number is listed in the third octet is a subnet number. However, now that we

have a subnet number in the fourth octet, we can subnet this octet just as we did with Class C subnetting. Let's try it out:
172.16.0.0 = Network address
255.255.255.192 = Subnet mask
1.Subnets? 210=1024
2.Hosts? 26-2=62
3.Valid subnets? 256 – 192 = 64. The subnets are shown in the following table. Do these numbers look familiar?
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the first eight subnet ranges, valid hosts, and broadcast addresses:

Subnet	0.0	0.64	0.128	0.192	1.0	1.64	1.128	1.192
First host	0.1	0.65	0.129	0.193	1.1	1.65	1.129	1.193
Last host	0.62	0.126	0.190	0.254	1.62	1.126	1.190	1.254
Broadcast	0.63	0.127	0.191	0.255	1.63	1.127	1.191	1.255

Practice Example 8B: 255.255.255.224 (/27)
This is done the same way as the preceding subnet mask, except that we just have more subnets and fewer hosts per subnet available.

172.16.0.0 = Network address
255.255.255.224 = Subnet mask
1.Subnets? 211=2048
2.Hosts? 25-2=30
3.Valid subnets? 256 – 224 = 32. 0, 32, 64, 96, 128, 160, 192, 224.
4.Broadcast address for each subnet?
5.Valid hosts?
The following table shows the first eight subnets:

Subnet	0.0	0.32	0.64	0.96	0.128	0.160	0.192	0.224
First host	0.1	0.33	0.65	0.97	0.129	0.161	0.193	0.225
Last host	0.30	0.62	0.94	0.126	0.158	0.190	0.222	0.254
Broadcast	0.31	0.63	0.95	0.127	0.159	0.191	0.223	0.255

This next table shows the last eight subnets:

Subnet	255.0	255.32	255.64	255.96	255.128	255.160	255.192	255.224
First host	255.1	255.33	255.65	255.97	255.129	255.161	255.193	255.225
Last host	255.30	255.62	255.94	255.126	255.158	255.190	255.222	255.254
Broadcast	255.31	255.63	255.95	255.127	255.159	255.191	255.223	255.255

Subnetting Class A Addresses

Class A subnetting is not performed any differently than Classes B and C, but there are 24 bits to play with instead of the 16 in a Class B address and the 8 in a Class C address.

Let's start by listing all the Class A masks:

```
255.0.0.0     (/8)
255.128.0.0   (/9)          255.255.240.0   (/20)
255.192.0.0   (/10)         255.255.248.0   (/21)
255.224.0.0   (/11)         255.255.252.0   (/22)
255.240.0.0   (/12)         255.255.254.0   (/23)
255.248.0.0   (/13)         255.255.255.0   (/24)
255.252.0.0   (/14)         255.255.255.128   (/25)
255.254.0.0   (/15)         255.255.255.192   (/26)
255.255.0.0   (/16)         255.255.255.224   (/27)
255.255.128.0   (/17)       255.255.255.240   (/28)
255.255.192.0   (/18)       255.255.255.248   (/29)
255.255.224.0   (/19)       255.255.255.252   (/30)
```

That's it. You must leave at least 2 bits for defining hosts. And I hope you can see the pattern by now. Remember, we're going to do this the same way as a Class B or C subnet. It's just that, again, we simply have more host bits and we just use the same subnet numbers we used with Class B and C, but we start using these numbers in the second octet.

Subnetting Practice Examples: Class A Addresses

When you look at an IP address and a subnet mask, you must be able to distinguish the bits used for subnets from the bits used for determining hosts. This is imperative

Practice Example 1A: 255.255.0.0 (/16)

Class A addresses use a default mask of 255.0.0.0, which leaves 22 bits for subnetting since you must leave 2 bits for host addressing. The 255.255.0.0 mask with a Class A address is using 8 subnet bits.

1. Subnets? 2^8=256
2.Hosts? 2^{16}-2=65,534
3.Valid subnets? What is the interesting octet? 256 – 255 = 1. 0, 1, 2, 3, etc. (all in the second octet).
The subnets would be 10.0.0.0, 10.1.0.0, 10.2.0.0, 10.3.0.0, etc., up to 10.255.0.0.
4.Broadcast address for each subnet?

5.Valid hosts?
The following table shows the first two and last two subnets, valid host range, and broadcast addresses for the private Class A 10.0.0.0 network:

Subnet	10.0.0.0	10.1.0.0	…	10.254.0.0	10.255.0.0
First host	10.0.0.1	10.1.0.1	…	10.254.0.1	10.255.0.1
Last host	10.0.255.254	10.1.255.254	…	10.254.255.254	10.255.255.254
Broadcast	10.0.255.255	10.1.255.255	…	10.254.255.255	10.255.255.255

I I.7 Static IP configuration

Static IP configuration requires passing computer to computer setting IP addresses. A Computer assigned an IP address in this way will hold it until the next change.

Steps

Start > Control panel > Network and internet connection> Network connection> Right click on Local area network > properties>Select Internet protocol (TCP/IP)> properties>Use the following IP address:

You have to set the IP address, the mask, and the default gateway.

I I.8 Automatic IP configuration-DHCP

DHCP short for Dynamic Host Configuration Protocol is a protocol which helps to dynamically assign IP addresses, instead of having static IP addresses. When a machine connects to a network it receive a IP address.

The server that manages this dynamically assigned IP addresses is called Dynamic Host Configuration Protocol (DHCP) server.

In these arrangements the workstations are called DHCP clients. The DHCP software resides both in the server and the workstation.

Installing the DHCP Service

1. Select start>Control Panel>Add or Remove Programs.
2. Click the Add/Remove windows components icon. The windows components wizard opens and lists all of the available components.
3. Select the Networking services item from the component list and click the Details button.
4. When the subcomponents of network services list appears, make sure Dynamic Host Configuration Protocol (DHCP) is selected and click the OK button.
5. Click the next button to continue the windows components wizard.
6. If prompted, enter the path to the windows server 2003 distribution files.
7. Click finish to close the windows components wizard. Close the Add or remove programs window.

Authorizing a DHCP Server in an active directory

1. Select start>Administrative tools>DHCP to open the DHCP snap-in.
2. Right-click the server you want to authorize and choose the authorize command.
3. Wait a short time to allow the authorization to take place.
4. Right-click the server again. Verify that the unauthorized command appears in the pop-up menu, this indicates that the server is now authorized.
5. Leave the window open for the next lab.

Several packets are sent between a DHCP server and a client machine:

- **DHCPDISCOVER** (to locate the available DHCP servers)
- **DHCPOFFER** (Response of the server on the packet DHCPDISCOVER, it contains the first parameters)
- **DHCPREQUEST** (Request of client for instance when it needs the extension of its lease)
- **DHCPACK** (Response of the server which contain the parameters and client IP address)
- **DHCPNAK** (Response of the server to indicate to the client that its lease period is expired or the client announce the bad network configuration)
- **DHCPDECLINE** (The client announce to the server that the address is already used)
- **DHCPRELEASE** (the client release its IP address)
- **DHCPINFORM** (The client asks the local parameters, he already has his IP address)

The first packet sent by a client is a DHCPDISCOVER. The server responds by DHCPOFFER, in particular for submitting an IP address to the client. A client establishes its configuration and delivers a DHCPREQUEST to validate its IP address (The request is in broadcast because DHCPOFFER doesn't have its own IP address). The server Answers simply with a DHCPACK with the IP address for confirming the delivery.

Lease

Lease a period of IP address validity, this period is set for the network resources optimization. When a client find that its IP lease is over, it may asks the server to extend its lease period.

I I.9 DNS configuration

A DNS (Domain Name Server) is a device (which is on your ISP) which associate an IP address to the address which easy to remember. For example the IP 207.68.137.65 is associated with http://www.microsoft.com in case you type that IP you will have the same result.

Steps for configuring a DNS

- Start > Control panel > Network and internet connection> Network connection> Right click on Local area network > properties>Select Internet protocol (TCP/IP)> properties>Use the following DNS server addresses.

I I.10 Router configuration

Definitions

-A router is a network device which connect networks and are more sophisticated than bridges and switches they work at the Network and Transport layers of the OSI model.

-Routers are a little slower than bridges because they take the time to make more intelligent decisions about how to route packets to other networks. For example, large networks are often logically divided into many smaller separate networks, and each small network is identified by a logical network address. These smaller networks are called subnetworks, or **subnets**. Each packet or frame, in addition to having a physical device address, also has a logical network or subnet address.

-A router can make decisions as to which neighboring network to send a packet to, based on its ultimate destination subnet address.

-Routers can be computers with operating systems and special network software, or they can be other dedicated devices built by network manufacturers.

Routers hold tables of network addresses, along with the best possible predetermined routes to these networks. These router tablescan also contain the cost of sending data to a network. The cost can be expressed in one of two ways:

Tick count: The time required for a packet to reach its destination. One tick equals 1/18 second.

Hop count: The number of routers a packet must pass through in order to reach its destination. (Hop count is the more common method of the two.)

The routing tables are modified every few minutes to reflect changes in the networks. When a router rebuilds its router table on the basis of new information, the process is Called route discovery.

Router configuration

Type the IP address of the router in the address bar. Type the login name and password. On the interface which opens you configure different settings on the router.

I I.11 Proxy configuration

A proxy server is a server which resides between a computer and another internet server with the function of filtering internet requests for the security purpose, ameliorate the performance, share connection between client machine and the server. It increases the speed of obtaining pages by creating a local database of the most accessed objects. In most cases proxy servers have integrated cache which allows navigating quickly the internet.

Functions of a proxy server are described below:

-When you try to connect to a web server, the browser sent the request to the cache server.

-Cache server (or proxy) verify if the page is not already stored on the disk of your computer, in case it is there it send directly to your computer in other case it asks the page to the web server.

-The web server sent the requested page and the cache server does the copy and stores it for the future request.

Having a proxy server present double interest:

-In 30% cases, the objects you load are delivered immediately because they exist on the cache server thus you gain time because pages are available quickly.

-It reduces the bandwidth you use on the internet because it allows you to access many pages.

Configuration on internet explorer French version 4.

-Choose format on the menu bar,

-Choose internet option,

-In the window which come find connection the click on configure,

-another window appear and type the following ULR :

http://www.univ-tln.fr/services/cri/cache.pac

-Click on ok and again ok. The configuration is over.

Summarized steps :

Tools->internet explorer->connections->LAN settings->write the proxy server address)

Chapter I II. Network tools

I II.1 Ping tool

Ping tool verify the IP connectivity of a computer using the TCP/IP protocol in sending messages. It counts in millseconds (ms) the necessary time for pachets to go the server and come back to the client.

This tool is used to solve connectivity, access and name resolution problems. The less the time in milliseconds is short the more is the speed of receiving and sending packets.

Example:

Ping www.yahoo.fr

I II.2 Tracet tool

Tracert tool not only allow to know the time used to send a packet to the serving and having it back, includes also the time it used from one node to another till it reaches the destination and come back.

Example: tracet www.yahoo.fr

I II.3 Netstart tool

Netstart tool (netsh.exe) helps to automate the start and stop of a service using commands.
Examples of its use:
Start a service
Net start name-of-a-service

Stop a service
Net stop name-of-a-service
Pause a service
Net pause name-of-a-service
Continue a service
Net continue name-of-a-service

I II.4 Winipcfg tool

Winipcfg tool is used on some Microsoft operating systems such as windows 95 and windows 98. Graphicaly it displays IP configuration information including the IP address, subnet mask, default gateway and DNS ip address.

I II.5 Ipconfig tool

Ipconfig tool is a tool which helps to display or change the computer IP address, mask, default gateway, and other settings

I II.6 WHOIS tool

Whois is a network tool that provide information about the owner of any second-level domain name who has registered it with Verisign (Verisign is a company which manages database which determine the interpretation of internet domain like .com and .net).

Whois can also be used to find out whether a domain name is available or has already been taken.

I II.7 Nslookup tool

Nslokup tool is a network tool which responds by default with the primary IP address associated with a domain specified. To query the primary address of about.com, for example:\>about.com

Adress: 67.215.65.132

Chapter IV . Internet, intranet, extrane0074

IV .1 Internet, intranet and extranet definition

- **The Internet** is a worldwide collection of computer networks, cooperating with each other to exchange data using a common software standard.

- **An intranet** is a private computer network that uses Internet Protocol technology to securely share any part of an organization's information or network operating system within that organization.

- **An extranet** is a computer network that allows controlled access from the outside, for specific business or educational purposes. An extranet can be viewed as an extension of a company's intranet that is extended to users outside the company, usually partners, vendors, and suppliers.

IV.1.1 Internet

The Internet is a worldwide collection of computer networks, cooperating with each other to exchange data using a common software standard. Through telephone wires and satellite links, Internet users can share information in a variety of forms.

Internet allows users to:

- connect easily through ordinary personal computers and local phone numbers;
- exchange electronic mail (E-mail) with friends and colleagues with accounts on the Internet;
- post information for others to access, and update it frequently;
- access multimedia information that includes sound, photographic images and even video; and
- access diverse perspectives from around the world.

The Internet began as ARPAnet, a U.S. Department of Defense project to create a nationwide computer network that would continue to function even if a large portion of it were destroyed in a nuclear war or natural disaster. The nature of the Internet changed abruptly in 1992, when the U.S. government began pulling out of network management, and commercial entities offered Internet access to the general public for the first time.

Information available on internet

Text documents, graphics files (digitized photographs and artwork), files that contain digitized sound and video.

Services

E-mail, for exchange of electronic mail messages.

USENET newsgroups (Interactive forums), for posting and responding to public "bulletin board" messages.

File Transfer Protocol (FTP), a system for storing and retrieving data files on large computer systems.

Gopher, a method of searching for various text-based Internet resources (largely obsolete).

TELNET, a way of connecting directly to computer systems on the Internet.

Internet Relay Chat (IRC), a system for sending public and private messages to other users in "real time"—that is, your message appears on the recipient's screen as soon as you type it.

CU-SeeMe, a videoconferencing system that allows users to send and receive sound and pictures simultaneously over the Internet.

The World Wide Web.

Download of software,

Chatsin which you and other users type (and, in some cases, speak) messages that are received by the chat participants instantly,

E-commerce,

E-learning,etc.

IV.1.2 Intranet

An intranet is a private computer network that uses Internet Protocol technology to securely share any part of an organization's information or network operating system within that organization.

Use of intranet

Intranets are being used to deliver tools and applications, e.g., collaboration (to facilitate working in groups and teleconferencing), sales and customer relationship management tools, project management etc., to advance productivity.

Benefits

Workers productivity: Intranets can help users to locate and view information faster and improve the services provided to the users.

Time: Intranets allow organizations to distribute information to employees on an as-needed basis;

Communication: Intranets can serve as powerful tools for communication within an organization, vertically and horizontally.

Business operations and management: Intranets are also being used as a platform for developing and deploying applications to support business operations and decisions across the internetworked enterprise.

Cost-effective: Users can view information and data via web-browser rather than maintaining physical documents such as procedure manuals, internal phone list and requisition forms. This can potentially save the business money on printing, duplicating documents

Enhance collaboration: Information is easily accessible by all authorized users, which enables teamwork.

Cross-platform capability: Standards-compliant web browsers are available for Windows, Mac, and UNIX.

Promote common corporate culture: Every user has the ability to view the same information within the Intranet.

Immediate updates: When dealing with the public in any capacity, laws, specifications, and parameters can change. Intranets make it possible to provide your audience with "live" changes so they are kept up-to-date, which can limit a company's liability.

IV.1.3 Extranet

An extranet is a computer network that allows controlled access from the outside, for specific business or educational purposes. An extranet can be viewed as an extension of a company's intranet that is extended to users outside the company, usually partners, vendors, and suppliers.

Advantages

Exchange large volumes of data using Electronic Data Interchange (EDI)

Share product catalogs exclusively with trade partners

Collaborate with other companies on joint development efforts

Jointly develop and use training programs with other companies

Provide or access services provided by one company to a group of other companies, such as an online banking application managed by one company on behalf of affiliated banks

Disadvantages

Extranets can be expensive to implement and maintain within an organization (e.g., hardware, software, employee training costs), if hosted internally rather than by an application service provider.

Security of extranets can be a concern when hosting valuable or proprietary information.

Difference between internet, intranet and extranet

1). Intranet is shared content accessed by members within a single organization.

Extranet is shared content accessed by groups through cross-enterprise boundaries.

Internet is global communication accessed through the Web.

2). The Internet, extranets, and intranets all rely on the same TCP/IP technologies.

However, they are different in terms of the levels of access they allow to various users inside and outside the organization and the size of the network.

An intranet allows for restricted access to only members of an organization;

an extranet expands that access by allowing non-members such as suppliers and customers to use company resources.

The difference between the Internet and extranets is that while the extranet allows limited access to non-members of an organization, the Internet generally allows everyone to access all network resources.

Similarities between intranet and extranet

Intranets and extranets all have three things in common:

They both use secured Internet access to the outside world.

Both can drastically save your company or organization a lot of money.

Both need a user ID & password to control access to the whole system.

Differences between intranet and extranet

An Intranet is owned by a single group while an Extranet extends to users outside the group

Intranet users have more access to resources than extranet users

Intranets do not usually go through the Internet while typical Extranets do

Intranets are easier to secure than Extranets

Chapter V . Internet connection

The technologies used to connect to the Internet are different than those used for connecting devices on local area network. DSL, cable modem and fiber provide fixed broadband Internet service, while WiMax and LTE additionally support mobile connectivity. In geographic areas where these high-speed options are unavailable, subscribers are forced to use older cellular services, satellite or even dial-up Internet instead.

- DSL vs. Cable Modem Internet
- Types of DSL
- T1 and T3 Lines
- Fiber Optic Cable
- LTE
- WiMax
- Satellite Internet
- Dial-up Internet

Before you create an Internet connection, check with your ISP to verify the required connection settings. A connection to your ISP may require one or more of the following settings:

- An account with an ISP including setup information.
- A phone number to call your ISP.
- A specific IP address.
- An IP address for the default gateway.
- DNS addresses and domain names.

With Network Connections, connecting to the Internet is easy. For example, to create a dial-up connection, you can use the following components to gain access to the Internet:

- The TCP/IP protocol that is enabled for your network connection.
- A modem or other connection to an Internet service provider (ISP).
- An account with an ISP.

Network connection types

There are five types of network: LAN, Virtual Private Network, Direct connections, Incoming connections and dial-up connections.

V .1 Internet service provider

An Internet service provider (ISP) is a company that provides Internet access. There are Internet service providers around the world. To connect to the Internet, you dial a phone number and log on to the remote system. Once connected, you have access to the Internet and any other services, such as e-mail, that are provided by the ISP. Fees usually apply for commercial ISPs.ISP present in Rwanda: MTN, TIGO, ARTEL.

V .2 Connect to the internet using a modem

A modem is a device that transmits data over telephone wires. The most common way to connect to the Internet is with a modem and an account with an Internet service provider (ISP).

Dial-up is an analog connection because data is sent over an analog, public telephone network. The modem converts received analog data to digital and vice versa. Because dial-up access uses normal telephone lines the quality of the connection is not always good and data rates are limited.

- Typical Dial-up connection speeds range from 2400 bps to 56 Kbps.

The following table describes the different types of:

Type	Explanation

28.8 or 56 kilobits per second (Kbps) modem	The most common way to connect to the Internet, internal modems plug into a PCI slot inside a computer. External modems plug into a serial, parallel, or USB port on a computer.
ISDN modem	ISDN is a high-speed digital line installed by a telephone company or telecommunications provider. ISDN connects to a regular phone line, and ISDN modems can be internal or external.
Cable modem	Cable modems use a broadband connection to the Internet through cable television infrastructure. These modems use frequencies that do not interfere with television transmission.
DSL modem	DSL modems use a broadband connection to the Internet through existing telephone lines, and can be internal or external. Internal DSL modems are plugged into an expansion slot in the computer and do not require a network adapter. External DSL modems use a network adapter to connect to the computer.

To make a dial-up connection to your workplace by using a phone line

1. Open Network Connections.
2. Under Network Tasks, click Create a new connection, and then click Next.
3. Click Connect to the network at my workplace, and then click Next.
4. Click Dial-up connection, click Next, and then follow the instructions in the New Connection Wizard.

V .3 Connect to internet using a wireless

Wireless Internet, or wireless broadband is one of the newest Internet connection types. Instead of using telephone or cable networks for your Internet connection, you use radio frequency bands. Wireless Internet provides an always-on connection which can be accessed from anywhere — as long as you geographically within a network coverage area.

To manually add a wireless network to the Preferred Networks list

1. Open Network Connections.
2. Click the wireless network connection icon, and then, in Network Tasks, click View available wireless networks.
3. Under Related Tasks on the left, click Change the order of preferred networks.
4. Click Add.
5. In Network name (SSID), type a name for the wireless network.
6. In Network Authentication, click an item in the list.
7. If this is a security-enabled network, in Data encryption, select the encryption method.
8. In Network key, type the network key, and then in Confirm network key, retype the key.

Note 1:

5. SSID stands for "service set identifier," and it is used to uniquely identify any given wireless network. We can also say that an ***SSID*** is a 32-character alphanumeric key uniquely identifying a wireless LAN.
6. **Wireless security** is the prevention of unauthorized access or damage to computers using wireless networks.

   The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be **cracked** in a few minutes with a basic laptop computer and widely available software tools.
   WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

   Note 2:

   - If the network that you are adding provides a network key automatically, make sure that the The key is provided for me automatically check box is selected.
   - If the wireless network that you are adding does not have an access point or a router, select thethis is a computer-to-computer (ad hoc) network; wireless access points are not used check box.
- For the network authentication method, we recommend that you choose Open. When the open method is combined with a wired equivalent privacy (WEP) network key, all network traffic is encrypted. If you choose Shared, a network key is still required, and even if you use a WEP network key, network traffic is not encrypted, which makes your network more vulnerable to intrusions.

V 4. xDSL

Refers collectively to all types of **d***igital* **s***ubscriber* **l***ines*, the two main categories being ADSL and SDSL. Two other types of xDSL technologies are *High-data-rate DSL (HDSL)* and *Very high DSL (VDSL).*

DSL technologies use sophisticated modulation schemes to pack data onto copper wires.

They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations.

xDSL is similar to ISDN inasmuch as both operate over existing copper telephone lines (POTS) and both require the short runs to a central telephone office (usually less than 20,000 feet). However, xDSL offers much higher speeds - up to 32 Mbps for upstream traffic, and from 32 Kbps to over 1 Mbps for downstream traffic.

Digital Subscriber Line (DSL) is a family of technologies that provides digital data transmission over the wires of a local telephone network.

This technology enables telephone companies to offer broadband service without major network rewiring and can be implemented quickly and profitably, especially because it stands to benefit both the consumer (with faster data rates) and the service providers (with new revenues from old cables). Here's how it works. Nearly all existing telephone lines can carry frequencies up to 1 MHz. But analog telephone service only requires a maximum frequency of 3.3 KHz, leaving a large amount of the bandwidth unused. xDSL makes use of this otherwise wasted space by piggybacking high-speed data traffic onto the unused bandwidth.

By filtering the frequencies at each end of this wide-open range (4 KHz to 2.2 MHz) and isolating them from the voice-bandwidth channel, the local telco can transport both traditional telephone signals and high-speed xDSL signals over the same old four-wire telephone line that already links your home or business to their central office (CO).

Other types

OC3

Short for Optical Carrier, level 3 it is used to specify the speed of fiber optic networks conforming to the SONET standard. OC3 is typically used as a fiber optic backbone for large networks with large voice, data, video, and traffic needs.

- Speeds are 155.52 Mbps, or roughly the speed of 100 T1 lines.

Satellite

Internet over Satellite (IoS) allows a user to access the Internet via a satellite that orbits the earth. A satellite is placed at a static point above the earth's surface, in a fixed position. Because of the enormous distances signals must travel from the earth up to the satellite and back again, IoS is slightly slower than high-speed terrestrial connections over copper or fiber optic cables.

Typical Internet over Satellite connection speeds (standard IP services) average around 492 up to 512 Kbps.

Chapter VI. Server management

Windows Server is a network manager that can function like a domain controller. It uses the controls of DHCP, DNS, and Active Directory to manage the network from the software side.

In this course we will use windows server 2003. Microsoft's Server 2003 is an operating system that functions in various capacities, Domain controller, DNS server, DHCP server, and Active Directory server. Each of these server operations helps manage the network that server 2003 is responsible for.

A domain controller

A Domain Controller is a computer that manages the network in several ways. The computer domain presents a collection of computers that are governed and controlled by the Domain Controller, a central server. This server has certain responsibilities to make sure the network is operating properly.

Domain controller differ from the Workgroup network on that a workgroup is a peer-to-peer type of network that has no central computer that acts like a network manager. Each computer can interact with the others provided that they are on the same subnet. If so, they can share files or network devices like printers.

The DNS Server

One of the functions of the Domain Controller is that network names and the IP addresses are resolved properly. Instead of using IP addresses there is a use of name resolution, the IP address is associated with a computer. That is what the DNS server routinely does.

The DHCP Server

The DHCP server performs leasing operations. It takes a group of IP addresses that have been created for the network and hands them out to computers that are joining the network. They are leased because, normally, the handout lasts 72 hours, and then it expires. However, it is typically renewed, so the same computer will receive the same IP address.

The other items that a DHCP server provides are the gateway, the subnet mask, and the IP address that belongs to the current DNS server, even if it belongs to the Domain Controller itself.

The gateway is a route to another network or to the DNS server. The subnet mask is a binary set of numbers that helps define what network the IP address belongs to.

Active directory

Active directory is an administrative tool designed to perform day-to-day Active Directory administration tasks. Active Directory is implemented on the Domain Controller and is used as the (software) manager on the computer

The administration tasks performed by the active directory include creating, deleting, modifying, moving, and setting permissions on objects stored in the directory.

These objects include organizational units, users, contacts, groups, computers, printers, and shared file objects.

The Active Directory tool is used for a variety of different management functions.

One function is to define who enters the network, both as a user or as a computer. Users are given login names and passwords and memberships to certain groups, like the administrators group. Computers are controlled with the DHCP server.

Another function involves Organizational Units. These are units where individuals are put into to control what they can and cannot access.

VI 1.User, account and password

With users divided in groups there is a need of control. For instance, a user might be a part of the IT department group, but not part of the Accounting department group. In this matter, the active directory will specify the security towards the network by controlling when a user can have access to the network. He will have an account created on him, login name and password.

VI .2 Permissions

Permissions are controls that make the network manageable in terms of the users, and computers, and the security privileges that are presented. It controls who can access the network, when, and what privileges are available.

One way is security. That means that users can only access the network if they have permission through a login and password account.

Another way is through computer control. This means that only certain devices can be part of the computer network. Adding a computer to the network means that controls on it come by way of the domain controller.

1. **What is Microsoft Active Directory?**

   Active Directory is Microsoft's directory service for the Windows architecture. It is a centralized and standardized system that automates network management of user data, security and distributed resources and enables interoperation with other directories.

   First introduced with Windows 2000 Server, Active Directory is designed especially for distributed networking environments, and provides a single hierarchical view from which to access and manage all network resources.

2. **What are the benefits of Active Directory over Windows NT 4.0 directory services?**

   Active Directory marked a shift in the way that Microsoft manages directory services, moving from the flat and fairly restrictive namespaces used by NT4 domains toward an actual hierarchical directory structure. There's a sample chapter from the Windows 2000

technical reference that provides a good introduction into the major differences between the NT4 and Active Directory directory services.

3. **What is the difference between Windows 2000 Active Directory and Windows 2003 Active Directory?**
   Windows 2003 Active Directory introduced a number of new security features, as well as convenience features such as the ability to rename a domain controller and even an entire domain. This article breaks down some of the key AD enhancements included with Windows Server 2003.

   The release of Windows Server 2003 SP1 included more improvements to Active Directory, including changes to default tombstone lifetimes, simpler troubleshooting and the ability to run domain controllers using virtualization technology.

4. **Is there any difference in Windows 2000 and 2003 group polices?**
   Windows Server 2003 introduced numerous changes to the default settings that can be affected by Group Policy. You can see a detailed list of each available setting and which OS is required to support it by downloading the Group Policy Settings Reference.
5. **What is the role of DNS in Active Directory?**
   Active Directory relies heavily on DNS (domain name system) to function, but not just any DNS. Active Directory is highly dependent on the Microsoft DNS service found on Windows server systems or equivalents. However, though not highly recommended, it *is* possible integrate a non-Microsoft DNS to use with Active Directory.

6. **When setting up a DNS server, can I give a DNS zone and an Active Directory domain the same name?**
   Not only *can* you, it's actually the preferred way to go if at all possible. You can install and configure DNS before installing Active Directory, or you can allow the Active Directory Installation Wizard (dcpromo) itself install DNS on your server in the background.

7. **How do I design two domains with DNS and Active Directory?**
   For Windows Server 2003, your best bet is going to be the Deployment Kit, which is available online from Microsoft's website. The section on "Deploying Network Services"

will assist you in designing and installing your DNS servers, and the section on "Designing and Deploying Directory and Security Services" will assist you with deploying Active Directory and configuring trust relationships.

8. **Why is replication important to Active Directory?**
   Replication is the process of sending update information for data that has changed in the directory to other domain controllers. It is key to the health and stability of an Active Directory environment, as without proper and timely replication, a domain will be unable to function effectively.

   There are three main elements or components that are replicated between domain controllers: the domain partition replica, the global catalog and the schema. It is important to have a firm understanding of replication and how it takes place, both within the domain and in multiple-site environments.

   For a more detailed explanation of how replication works in AD, see our Active Directory replication guide.

9. **Are there any security best practices for Active Directory design?**
   Layered security is the best method to use when planning and designing a security solution. This involves placing your valued assets at the center of your environment and building or deploying multiple concentric circles or rings of protection around those assets. Thus, violations to confidentiality, integrity, or availability must overcome numerous security restrictions, precautions and protections before being able to affect your assets.

   While Microsoft has increased the default security within Active Directory for Windows Server 2003 and 2008 installations, you still need to consider additional security settings after it is installed. This tutorial provides more security best practices for Active Directory.

10. **What's new in Active Directory for Windows Server 2008?**
    Windows 2008 Active Directory includes several new features, including read-only domain controllers, new roles for Server Core and a restartable AD.

4.6. Addressing

4.6. 1. NIC AND THE MAC ADDRESS

To be connected to a LAN, each computer must have an adapter card known as **Network Interface Card (NIC**) which provides physical connection of the computer to the network. Each NIC installed in a computer has serial number which is the unique identifier of this computer among others on the network. This number is also called **Media Access Control (MAC) Address** or the **physical address**. This address is assigned to the NIC by the manufacturer at the time of manufacturing. This address is stored in the ROM of the NIC and that's why it is called ***burned-in addresses***.

MAC addresses are **48 bits in length** and are expressed as **12 hexadecimal digits**. The **first 6** hexadecimal digits identify the manufacturer and thus comprise the **Organizational Unique Identifier (OUI)**. The **last 6** hexadecimal digits comprise the **interface serial number**.

4.6. 2. IP ADDRESS

TCP/IP suite of protocols requires that to be connected to internet, each computer must be assigned a **unique computer name** and a **unique numeric address** known as **IP Address** (**Internet Protocol Address**). If a computer has multiple network adapters, each adapter will have its own IP address.

IP addresses are considered as 32 bit numbers because their binary value occupies 32 positions. Since each of the eight positions can have two different states (1 or 0) the total number of possible combinations per octet is 2^8 or 255. An IP address is 32 bit long making each of the 8bit numbers separated by periods. To make it easier for humans to remember IP addresses, the IP addresses are expressed in decimal format while the computers communicate in binary form

Example: Decimal format:216.27.61.137

Binary format:-11011000.00011011.0011101.10001001

TCP/IP enables packets of data to traverse many networks to arrive at their destination.

When an organization applies for IP address Internet Corporation for Assigned Names and Numbers **(ICANN)** assigns a range of addresses appropriate to the number of hosts on the organization network. This role was assumed by the **InterNIC (Internet Network Information Center)** up to 1998.

An IP address contains two pieces of Information:

- **Host ID** which identifies the host (computer, printer, switch, etc.)
- **Network ID** which identifies the network to which the host is attached.

When the computer is moved to a different subnet work the IP address must be changed to reflect the new subnet ID.

On TCP/IP network, messages are broken up into small pieces of data, called **packets**, before they are transmitted over a network. This process allows for error checking and easier retransmission if the packet is lost or corrupted. Address information is added to the beginning and to the end of packets before they are transmitted. The packet, along with the address information, is called a **frame**.

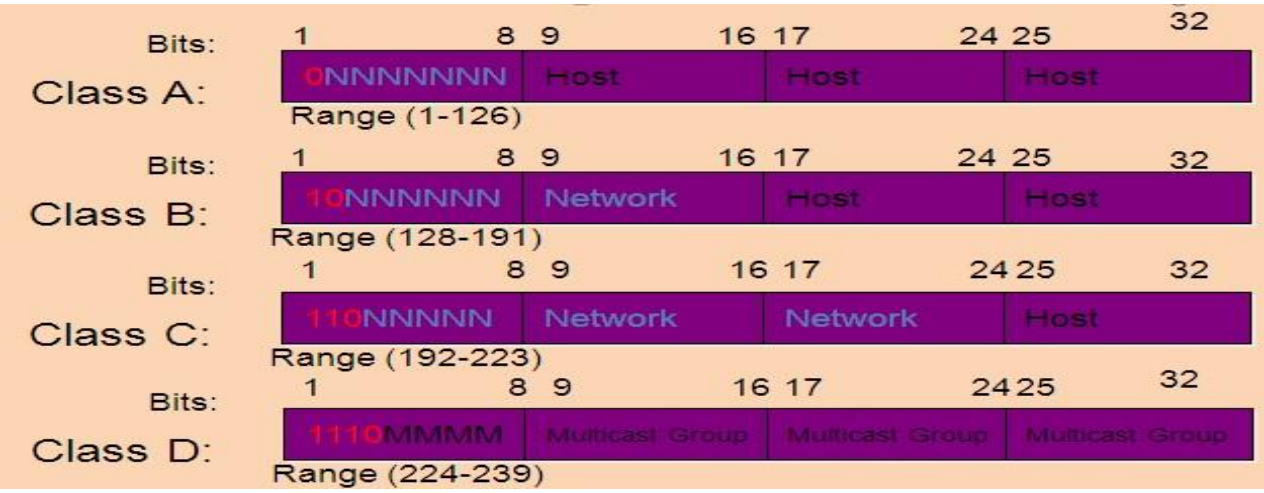
A computer connected to the TCP/IP network uses the network ID and host ID to determine which packets it should receive or ignore.

The Internet community has defined address classes to accommodate networks of varying sizes.

Those classes of IP Addresses are the following:

- **Class A**
- **Class B**
- **Class C**
- **Class D : multicast**
- **Class E : reserved**

CLASSES AND RANGES OF THEIR IP ADDRESSES



Class A is assigned to very large Networks, such as major international companies. In the class A, the first octet is reserved for the network address. The most left bit must be turned to 0. The remaining 7 bits will be used to assign a network address. Each bit can either be 0 or 1. The smallest number will be 0 and the biggest one is 127. There are 128 numbers, equivalent to 2^7. Since 0 and 127 cannot be assigned as a network addresses, the number of networks in class A is $2^N-2=2^7-2=126$ networks, i.e. 126 addresses. N is the number of bits reserved for the network ID part.

The other three octets on the right of the IP can be used for host addresses that identify each host on this network. There are 24 bits. Each of these bits can either be 0 or 1, but all of them will neither be 0 nor 1 at the same time. Turning all bits at 0 makes the IP Address becoming the network ID. Turning all bits at one gives a special IP Address called a **broadcast address** and it cannot be assigned to any host. That's why the number of hosts in the class A is $2^N-2=2^{24}2=16777214$ hosts per network. N is the number of bits reserved for the host ID part.

An example of an IP Address of class A is **10.12.13.19**. In this IP Address, the network ID is **10.0.0.0** and the host ID is **0.12.13.19**

Class B is used for the medium sized networks. In the class B, the first two octets are reserved for the network address. The first most left bit is 1 and the second most left bit is 0 (by convention). The remaining 14 bits will be used to assign a network address. Each bit can either be 0 or 1.

Considering the first octet, if all of the remaining 6 bits are zeros, the equivalent decimal number is 128. If all of the six bits are ones, the equivalent decimal number is 191. That's why any IP Address with the first octet is in the range of 128 to 191 is in class B.

The number of networks in class B is $2^N=2^{14}$= 16,384 networks, i.e. 16,384 addresses. N is the number of bits reserved for the network ID part.

The other two octets remaining are used for host addresses that identify each host on this network. There are 16 bits. Each of these bits can either be 0 or 1, but all of them will neither be 0 at the same time nor 1 at the same time. That's why the number of hosts per a network of class B is $2^N-2=2^{16}-2$=65532 hosts or addresses per network.

An example of an IP Address of class B is **190.12.13.19**. In this IP Address, the network ID is **190.12.0.0** and the host ID is **0.0.13.19**

Class C addresses are commonly used for small to mid- size networks.

In the class C, the first three octets are reserved for the network ID. The first most left bit is 1, the second most left bit is 1 and the third most left bit is 0 (by convention). The remaining 21 bits (5 bits for the first octets, 8 bits for the second octets and 8 bits for the third octets) will be used to assign a network address. Each bit can either be 0 or 1.

Considering the first octet, if all of the remaining 5 bits are zeros, the equivalent decimal number is 192. If all of the 5 bits are ones, the equivalent decimal number is 223. That's why any IP Address with the first octet is in the range of 192 to 223 is in class C.

The number of networks in class C is $2^N=2^{21}$= 2,097,152networks, i.e. 2,097,152addresses. N is the number of bits reserved for the network ID part.

The other one octet remaining is used for host addresses that identify each host on this network. There are 8 bits. Each of these bits can either be 0 or 1, but all of them will neither be 0 at the same time nor 1 at the same time. That's why the number of hosts per a network of class C is $2^N2=2^8-2$= 254 hosts or addresses per network.

An example of an IP Address of class C is **199.12.13.19**. In this IP Address, the network ID is

199.12.13.0 and the host ID is **0.0.0.19**

EXERCISE: COMPLETE THE FOLLOWING TABLE

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			

ANSWER

Address	Class	Network ID	Host ID
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16

Giving an IP Address to a computer

A computer can get an IP Address manually or automatically (from a DHCP server).

- Manually

To receive and deliver packets successfully between computers, TCP/IP requires that the network administrator provide three values:

a. **IP address**
b. **Subnet mask**
c. **Default gateway (router)**

A subnet mask is a 32 bit value that allows the recipient of a frame to distinguish the network ID portion of an IP Address from the host ID.

A subnet mask is created by assigning 1's to network ID bits and 0's to host ID bits. The 32 bit number is then converted to a dotted decimal notation.

For each IP Address of a class A network, the subnet mask will be:

11111111.00000000.00000000.00000000 (binary format) which is **255.0.0.0 (decimal format)** For each IP Address of a class B network, the subnet mask will be:

11111111. 11111111.00000000.00000000 (binary format) which is **255. 255.0.0 (decimal format)**

For each IP Address of a class C network, the subnet mask will be:

11111111. 11111111. 11111111.00000000 (binary format) which is **255. 255. 255.0 (decimal format)**

A default gateway is the device that passes traffic from the local subnet to devices on other subnets. *The default gateway often connects a local network to the Internet*, although internal gateways for local networks also exist. Normally, that device is a **router**.

Steps to give an IP Address to a computer connected to a LAN (manually)

- *Right-click the "My network places" icon*
- *Click Properties*
- *Right-click the "Local Area Connection" icon*
- *Click Properties*
- *On the dialog box, click the "General" tab*
- *Under "This connection uses the following items:" box, scroll through the list and click "Internet Protocol (TCP/IP)"*

- *Click "Properties" button*
- *On the dialog box, click the "General" tab*
- *Select the "Use the following IP Address:" radio button*
- *Now start filling in the IP Address, subnet mask and default gateway*
- *If there is a DNS server address you know, select the "Use the following DNS server addresses" radio button and start filling in their IP Addresses, otherwise go to the next step*
- *Click OK*
- *Click OK*

➢ Automatically

Another way a computer can get an IP Address is from a **DHCP** (Dynamic Host Configuration Protocol) server automatically. This server uses a protocol called DHCP which allows a computer to be configured automatically, eliminating the need for intervention by a network administrator. DHCP server offers ***dynamic configuration of IP addresses and related information***.

Allowing a computer to get an IP Address from a DHCP server prevents two computers from accidentally being configured with the same IP address.

To allow the computer connected to a TCP/IP network to get dynamic configuration of IP Address, follow these steps:

- *Right-click the "My network places" icon*
- *Click Properties*
- *Right-click the "Local Area Connection" icon*
- *Click Properties*
- *On the dialog box, click the "General" tab*
- *Under "This connection uses the following items:" box, scroll through the list and click "Internet Protocol (TCP/IP)"*
- *Click "Properties" button*

- *On the dialog box, click the "General" tab*
- *Select the "Obtain IP Address automatically" radio button*
- *Click OK*
- *Click OK again*